Códigos electrónicos

Código de Derecho de la Ciberseguridad

Edición actualizada a 2 de abril de 2025

INCIBE

BOLETÍN OFICIAL DEL ESTADO

La última versión de este Código en PDF y ePUB está disponible para su descarga **gratuita** en:
www.boe.es/biblioteca_juridica/

Alertas de actualización en Mi BOE: www.boe.es/mi_boe/

Para adquirir el Código en formato papel: tienda.boe.es

Esta obra está sujeta a licencia Creative Commons de Reconocimiento-NoComercial-SinObraDerivada 4.0 Internacional, (CC BY-NC-ND 4.0).

© Instituto Nacional de Ciberseguridad
© Agencia Estatal Boletín Oficial del Estado
NIPO (PDF): 007-16-125-9
NIPO (Papel): 007-16-124-3
NIPO (ePUB): 007-16-126-4
ISBN: 978-84-340-2330-7
Depósito Legal: M-25852-2016

Catálogo de Publicaciones de la Administración General del Estado
cpage.mpr.gob.es

Agencia Estatal Boletín Oficial del Estado
Avenida de Manoteras, 54
28050 MADRID
www.boe.es

SUMARIO

§ 1. Nota del autor 1

CONSTITUCIÓN ESPAÑOLA

§ 2. Constitución Española. [Inclusión parcial] 6

NORMATIVA DE SEGURIDAD NACIONAL

§ 3. Ley 36/2015, de 28 de septiembre, de Seguridad Nacional 8

§ 4. Orden PRA/33/2018, de 22 de enero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se regula el Consejo Nacional de Ciberseguridad 19

§ 5. Orden PRA/116/2017, de 9 de febrero, por la que se publica el Acuerdo del Consejo Seguridad Nacional de implementación de los mecanismos para garantizar el funcionamiento integrado del Sistema de Seguridad Nacional 24

§ 6. Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad . . . 29

§ 7. Orden PRE/2740/2007, de 19 de septiembre, por la que se aprueba el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información 105

§ 8. Orden ESS/775/2014, de 7 de mayo, por la que se crea el Comité de Seguridad de los Sistemas de Información de la Seguridad Social 145

§ 9. Orden TES/369/2023, de 10 de abril, por la que se aprueba la Política de Seguridad de la Información y de los Servicios en el ámbito de la administración digital del Ministerio de Trabajo y Economía Social y se crea el Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Departamento 148

§ 10. Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica 161

§ 11. Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información 180

§ 12. Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información 201

§ 13. Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia 226

§ 14. Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia 234

§ 15. Ley 9/1968, de 5 de abril, sobre secretos oficiales 238

§ 16. Decreto 242/1969, de 20 de febrero, por el que se desarrollan las disposiciones de la Ley 9/1968, de 5 de abril sobre Secretos Oficiales 242

§ 17. Ley Orgánica 4/1981, de 1 de junio, de los estados de alarma, excepción y sitio 251

§ 18. Ley 1/2019, de 20 de febrero, de Secretos Empresariales 259

§ 19. Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional 273

§ 20. Real Decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021 291

§ 21. Orden ISM/1320/2024, de 18 de noviembre, por la que se aprueba la Política de Seguridad de la Información del Ministerio de Inclusión, Seguridad Social y Migraciones y se crea el Comité de Seguridad de los Sistemas de Información 322

INFRAESTRUCTURAS CRÍTICAS

§ 22. Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas 336

§ 23. Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas 347

§ 24. Resolución de 8 de septiembre de 2015, de la Secretaría de Estado de Seguridad, por la que se aprueban los nuevos contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos 365

NORMATIVA DE SEGURIDAD

§ 25. Orden INT/859/2023, de 21 de julio, por la que se desarrolla la estructura orgánica y funciones de los servicios centrales y territoriales de la Dirección General de la Policía. [Inclusión parcial] 384

§ 26. Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana 388

§ 27. Ley 5/2014, de 4 de abril, de Seguridad Privada 416

§ 28. Real Decreto 2364/1994, de 9 de diciembre, por el que se aprueba el Reglamento de Seguridad Privada 464

EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD

§ 29. Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. [Inclusión parcial] 533

§ 30. Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional 535

§ 31. Real Decreto 521/2020, de 19 de mayo, por el que se establece la organización básica de las Fuerzas Armadas. [Inclusión parcial] 538

§ 32. Orden DEF/710/2020, de 27 de julio, por la que se desarrolla la organización básica del Estado Mayor de la Defensa. [Inclusión parcial] 540

TELECOMUNICACIONES Y USUARIOS

§ 33. Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico 542

§ 34. Real Decreto 381/2015, de 14 de mayo, por el que se establecen medidas contra el tráfico no permitido y el tráfico irregular con fines fraudulentos en comunicaciones electrónicas 575

§ 35. Orden TDF/149/2025, de 12 de febrero, por la que se establecen medidas para combatir las estafas de suplantación de identidad a través de llamadas telefónicas y mensajes de texto fraudulentos y para garantizar la identificación de la numeración utilizada para la prestación de servicios de atención al cliente y realización de llamadas comerciales no solicitadas 584

§ 36. Real Decreto 1163/2005, de 30 de septiembre, por el que se regula el distintivo público de confianza en los servicios de la sociedad de la información y de comercio electrónico, así como los requisitos y el procedimiento de concesión 592

§ 37. Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos 601

§ 38. Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza 653

§ 39. Ley 9/2014, de 9 de mayo, General de Telecomunicaciones. [Inclusión parcial] 672

§ 40. Ley 11/2022, de 28 de junio, General de Telecomunicaciones 676

§ 41. Real Decreto 123/2017, de 24 de febrero, por el que se aprueba el Reglamento sobre el uso del dominio público radioeléctrico 816

§ 42. Real Decreto 1066/2001, de 28 de septiembre, por el que se aprueba el Reglamento que establece condiciones de protección del dominio público radioeléctrico, restricciones a las emisiones radioeléctricas y medidas de protección sanitaria frente a emisiones radioeléctricas 878

§ 43. Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones 892

§ 44. Orden PRE/199/2013, de 29 de enero, por la que se define el formato de entrega de los datos conservados por los operadores de servicios de comunicaciones electrónicas o de redes públicas de comunicaciones a los agentes facultados 903

§ 45. Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación 907

§ 46. Real Decreto 443/2024, de 30 de abril, por el que se aprueba el Esquema Nacional de Seguridad de redes y servicios 5G 925

§ 47. Real Decreto 255/2025, de 1 de abril, por el que se regula el Documento Nacional de Identidad . . . 970

CIBERDELINCUENCIA

§ 48. Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. [Inclusión parcial] 981

§ 49. Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores. [Inclusión parcial] 1014

§ 50. Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal. [Inclusión parcial] 1023

PROTECCIÓN DE DATOS

§ 51. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales 1068

§ 52. Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal 1130

§ 53. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) 1183

§ 54. Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. [Inclusión parcial] 1273

RELACIONES CON LA ADMINISTRACIÓN

§ 55. Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. [Inclusión parcial] 1311

§ 56. Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. [Inclusión parcial] 1320

ÍNDICE SISTEMÁTICO

§ 1. Nota del autor 1

CONSTITUCIÓN ESPAÑOLA

§ 2. Constitución Española. [Inclusión parcial] 6

[. . .]

TÍTULO I. De los derechos y deberes fundamentales 6

[. . .]

CAPÍTULO SEGUNDO. Derechos y libertades 6
Sección 1.ª De los derechos fundamentales y de las libertades públicas 6

[. . .]

CAPÍTULO TERCERO. De los principios rectores de la política social y económica 7

[. . .]

NORMATIVA DE SEGURIDAD NACIONAL

§ 3. Ley 36/2015, de 28 de septiembre, de Seguridad Nacional 8

Preámbulo 8
TÍTULO PRELIMINAR. Disposiciones generales 10
TÍTULO I. Órganos competentes de la Seguridad Nacional 12
TÍTULO II. Sistema de Seguridad Nacional 13
TÍTULO III. Gestión de crisis en el marco del Sistema de Seguridad Nacional 15
TÍTULO IV. Contribución de recursos a la Seguridad Nacional 16
Disposiciones adicionales 17
Disposiciones transitorias 18
Disposiciones finales 18

§ 4. Orden PRA/33/2018, de 22 de enero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se regula el Consejo Nacional de Ciberseguridad 19

Parte dispositiva 19
ANEJO. Acuerdo por el que se regula el Consejo Nacional de Ciberseguridad 19
ANEXO. Acuerdo por el que se regula el Consejo Nacional de Ciberseguridad 20

§ 5. Orden PRA/116/2017, de 9 de febrero, por la que se publica el Acuerdo del Consejo Seguridad Nacional de implementación de los mecanismos para garantizar el funcionamiento integrado del Sistema de Seguridad Nacional 24

Parte dispositiva 24
ANEJO. Acuerdo de implementación de los mecanismos para garantizar el funcionamiento integrado del Sistema de Seguridad Nacional 24
Preámbulo 24
Artículos 26

ANEXO. Acuerdo de implementación de los mecanismos para garantizar el funcionamiento integrado del Sistema de Seguridad Nacional . . . 26

§ 6. Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. . . . 29

Preámbulo . . . 29
CAPÍTULO I. Disposiciones generales . . . 36
CAPÍTULO II. Principios básicos . . . 37
CAPÍTULO III. Política de seguridad y requisitos mínimos de seguridad . . . 39
CAPÍTULO IV. Seguridad de los sistemas: auditoría, informe e incidentes de seguridad . . . 45
CAPÍTULO V. Normas de conformidad . . . 47
CAPÍTULO VI. Actualización del Esquema Nacional de Seguridad . . . 48
CAPÍTULO VII. Categorización de los sistemas de información . . . 48
Disposiciones adicionales . . . 49
Disposiciones transitorias . . . 49
Disposiciones derogatorias . . . 49
Disposiciones finales . . . 50
ANEXO I. Categorías de seguridad de los sistemas de información . . . 50
ANEXO II. Medidas de Seguridad . . . 52
ANEXO III. Auditoría de la seguridad . . . 100
ANEXO IV. Glosario . . . 101

§ 7. Orden PRE/2740/2007, de 19 de septiembre, por la que se aprueba el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información. . . . 105

Preámbulo . . . 105
Artículos . . . 106
Disposiciones adicionales . . . 106
Disposiciones finales . . . 106
REGLAMENTO DE EVALUACIÓN Y CERTIFICACIÓN DE LA SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN . . . 107
CAPÍTULO I. Disposiciones generales . . . 107
CAPÍTULO II. Estructura y funciones del organismo de certificación . . . 108
Sección 1.ª Estructura del organismo de certificación . . . 108
Sección 2.ª Funciones de los cargos del organismo de certificación . . . 109
Sección 3.ª Consejo de acreditación y certificación . . . 111
Sección 4.ª Acreditación y certificación . . . 112
CAPÍTULO III. Requisitos de acreditación de laboratorios . . . 112
Sección 1.ª Requisitos de seguridad para laboratorios que evalúen productos clasificados . . . 113
Sección 2.ª Requisitos de seguridad para laboratorios que evalúen productos no clasificados . . . 113
Subsección 1.ª Responsabilidades del laboratorio . . . 113
Subsección 2.ª Tratamiento de la información de las evaluaciones . . . 115
Subsección 3.ª Servicio de Protección de la información de las evaluaciones . . . 117
Subsección 4.ª Inspecciones de seguridad . . . 118
Subsección 5.ª Visitas . . . 119
Subsección 6.ª Zonas de acceso restringido . . . 120
Subsección 7.ª Procedimiento de seguridad . . . 121
Subsección 8.ª Seguridad de los sistemas de información . . . 122
Sección 3.ª Requisitos de los procedimientos de evaluación . . . 124
CAPÍTULO IV. Acreditación de laboratorios . . . 127
Sección 1.ª Acreditación . . . 127
Sección 2.ª Alcance de la acreditación . . . 127
Sección 3.ª Criterios de acreditación . . . 128
Sección 4.ª Procedimiento de acreditación . . . 128
Sección 5.ª Seguimiento de la actividad de evaluación . . . 131
Sección 6.ª Formulación de observaciones, plazos y recursos . . . 132
CAPÍTULO V. Certificación de productos y sistemas . . . 133
Sección 1.ª Certificación . . . 133
Sección 2.ª Alcance de la certificación . . . 134
Sección 3.ª Criterios de certificación . . . 134
Sección 4.ª Procedimiento de certificación . . . 134
Sección 5.ª Seguimiento del uso de los certificados . . . 137
Sección 6.ª Formulación de observaciones, plazos y recursos . . . 138
CAPÍTULO VI. Criterios y metodologías de evaluación . . . 139

CAPÍTULO VII. Uso de la condición de laboratorio acreditado y de producto certificado 140

§ 8. Orden ESS/775/2014, de 7 de mayo, por la que se crea el Comité de Seguridad de los Sistemas de Información de la Seguridad Social 145

Preámbulo 145
Artículos 146
Disposiciones adicionales 147
Disposiciones finales 147

§ 9. Orden TES/369/2023, de 10 de abril, por la que se aprueba la Política de Seguridad de la Información y de los Servicios en el ámbito de la administración digital del Ministerio de Trabajo y Economía Social y se crea el Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Departamento 148

Preámbulo 148
Artículos 149
Disposiciones adicionales 160
Disposiciones derogatorias 160
Disposiciones finales 160

§ 10. Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica 161

Preámbulo 161
CAPÍTULO I. Disposiciones generales 163
CAPÍTULO II. Principios básicos 164
CAPÍTULO III. Interoperabilidad organizativa 164
CAPÍTULO IV. Interoperabilidad semántica 165
CAPÍTULO V. Interoperabilidad técnica 166
CAPÍTULO VI. Infraestructuras y servicios comunes 167
CAPÍTULO VII. Comunicaciones de las Administraciones públicas 167
CAPÍTULO VIII. Reutilización y transferencia de tecnología 168
CAPÍTULO IX. Firma electrónica y certificados 169
CAPÍTULO X. Recuperación y conservación del documento electrónico 170
CAPÍTULO XI. Normas de conformidad 172
CAPÍTULO XII. Actualización 173
Disposiciones adicionales 173
Disposiciones transitorias 176
Disposiciones derogatorias 176
Disposiciones finales 176
ANEXO. Glosario de términos 176

§ 11. Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información 180

Preámbulo 180
TÍTULO I. Disposiciones generales 184
TÍTULO II. Servicios esenciales y servicios digitales 186
TÍTULO III. Marco estratégico e institucional 187
TÍTULO IV. Obligaciones de seguridad 190
TÍTULO V. Notificación de incidentes 192
TÍTULO VI. Supervisión 195
TÍTULO VII. Régimen sancionador 196
Disposiciones adicionales 199
Disposiciones finales 200

§ 12. Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información 201

Preámbulo 201
CAPÍTULO I. Disposiciones generales 203
CAPÍTULO II. Marco estratégico e institucional 204
CAPÍTULO III. Requisitos de seguridad 207

CAPÍTULO IV. Gestión de incidentes de seguridad . . . 209
CAPÍTULO V. Supervisión . . . 212
Disposiciones adicionales . . . 213
Disposiciones transitorias . . . 214
Disposiciones finales . . . 214
ANEXO. Instrucción nacional de notificación y gestión de ciberincidentes . . . 215

§ 13. Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia . . . 226

Preámbulo . . . 226
CAPÍTULO I. Disposiciones generales . . . 227
CAPÍTULO II. De la organización y régimen jurídico . . . 229
CAPÍTULO III. Del control . . . 231
Disposiciones adicionales . . . 232
Disposiciones transitorias . . . 232
Disposiciones derogatorias . . . 232
Disposiciones finales . . . 232

§ 14. Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia . . . 234

Preámbulo . . . 234
Artículos . . . 235
Disposiciones adicionales . . . 235
Disposiciones finales . . . 237

§ 15. Ley 9/1968, de 5 de abril, sobre secretos oficiales . . . 238

Preámbulo . . . 238
Artículos . . . 239
DISPOSICIÓN FINAL . . . 241

§ 16. Decreto 242/1969, de 20 de febrero, por el que se desarrollan las disposiciones de la Ley 9/1968, de 5 de abril sobre Secretos Oficiales . . . 242

Preámbulo . . . 242
Artículos . . . 242
Disposiciones adicionales . . . 250

§ 17. Ley Orgánica 4/1981, de 1 de junio, de los estados de alarma, excepción y sitio . . . 251

Preámbulo . . . 251
CAPÍTULO PRIMERO. Disposiciones comunes a los tres estados . . . 251
CAPÍTULO II. El estado de alarma . . . 252
CAPÍTULO III. El estado de excepción . . . 253
CAPÍTULO IV. El estado de sitio . . . 257
DISPOSICIÓN DEROGATORIA . . . 258
DISPOSICIÓN FINAL . . . 258

§ 18. Ley 1/2019, de 20 de febrero, de Secretos Empresariales . . . 259

Preámbulo . . . 259
CAPÍTULO I. Disposiciones generales . . . 262
CAPÍTULO II. Obtención, utilización y revelación de secretos empresariales . . . 263
CAPÍTULO III. El secreto empresarial como objeto del derecho de propiedad . . . 264
CAPÍTULO IV. Acciones de defensa de los secretos empresariales . . . 265
CAPÍTULO V. Jurisdicción y normas procesales . . . 267
Sección 1.ª Disposiciones generales . . . 267
Sección 2.ª Diligencias para la preparación del ejercicio de acciones de defensa de los secretos empresariales 269
Sección 3.ª Medidas cautelares . . . 269
Disposiciones transitorias . . . 270
Disposiciones finales . . . 270

§ 19. Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional . . . 273

Parte dispositiva . . . 273
ANEXO. Estrategia Nacional de Ciberseguridad 2019 . . . 273
Resumen ejecutivo . . . 274
Introducción . . . 275
CAPÍTULO 1. El ciberespacio como espacio común global . . . 276
CAPÍTULO 2. Las amenazas y desafíos en el ciberespacio . . . 278
CAPÍTULO 3. Propósito, principios y objetivos para la ciberseguridad . . . 280
CAPÍTULO 4. Líneas de acción y medidas . . . 284
CAPÍTULO 5. La ciberseguridad en el Sistema de Seguridad Nacional . . . 288

§ 20. Real Decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021 . . . 291

Preámbulo . . . 291
Artículos . . . 292
Disposiciones derogatorias . . . 292
Disposiciones finales . . . 292
ESTRATEGIA DE SEGURIDAD NACIONAL 2021 . . . 292
CAPÍTULO 1. Seguridad global y vectores de transformación . . . 295
CAPÍTULO 2. Una España segura y resiliente . . . 299
CAPÍTULO 3. Riesgos y amenazas . . . 302
CAPÍTULO 4. Un planeamiento estratégico integrado . . . 309
CAPÍTULO 5. El Sistema de Seguridad Nacional y la Gestión de Crisis . . . 319

§ 21. Orden ISM/1320/2024, de 18 de noviembre, por la que se aprueba la Política de Seguridad de la Información del Ministerio de Inclusión, Seguridad Social y Migraciones y se crea el Comité de Seguridad de los Sistemas de Información . . . 322

Preámbulo . . . 322
Artículos . . . 324
Disposiciones adicionales . . . 334
Disposiciones derogatorias . . . 334
Disposiciones finales . . . 335

INFRAESTRUCTURAS CRÍTICAS

§ 22. Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas . . . 336

Preámbulo . . . 336
TÍTULO I. Disposiciones generales . . . 338
TÍTULO II. El Sistema de Protección de Infraestructuras Críticas . . . 340
TÍTULO III. Instrumentos y comunicación del Sistema . . . 343
Disposiciones adicionales . . . 344
Disposiciones finales . . . 345
ANEXO. Sectores estratégicos y Ministerios/Organismos del sistema competentes . . . 346

§ 23. Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas . . . 347

Preámbulo . . . 347
TÍTULO I . . . 348
Disposiciones transitorias . . . 348
Disposiciones finales . . . 348
REGLAMENTO DE PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS . . . 349
TÍTULO I. Disposiciones generales . . . 349
CAPÍTULO I. Objeto y ámbito de aplicación . . . 349
CAPÍTULO II. El Catálogo Nacional de Infraestructuras Estratégicas . . . 349
TÍTULO II. Los agentes del Sistema de Protección de Infraestructuras Críticas . . . 350

TÍTULO III. Instrumentos de planificación . . . 357
CAPÍTULO I. El Plan Nacional de Protección de las Infraestructuras Críticas . . . 357
CAPÍTULO II. Los Planes Estratégicos Sectoriales . . . 358
CAPÍTULO III. Los Planes de Seguridad del Operador . . . 359
CAPÍTULO IV. Los Planes de Protección Específicos . . . 360
CAPÍTULO V. Los Planes de Apoyo Operativo . . . 362
TÍTULO IV. Comunicaciones entre los operadores críticos y las Administraciones públicas . . . 363

§ 24. Resolución de 8 de septiembre de 2015, de la Secretaría de Estado de Seguridad, por la que se aprueban los nuevos contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos . . . 365

Parte dispositiva . . . 365
ANEXO I. Guía Contenidos Mínimos . . . 366
ANEXO II. Guía de contenidos mínimos . . . 375

NORMATIVA DE SEGURIDAD

§ 25. Orden INT/859/2023, de 21 de julio, por la que se desarrolla la estructura orgánica y funciones de los servicios centrales y territoriales de la Dirección General de la Policía. [Inclusión parcial] . . . 384

[. . .]

CAPÍTULO II. Organización central . . . 384
Sección 1.ª Dirección General de la Policía . . . 384

[. . .]

[. . .]

§ 26. Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana . . . 388

Preámbulo . . . 388
CAPÍTULO I. Disposiciones generales . . . 392
CAPÍTULO II. Documentación e identificación personal . . . 395
CAPÍTULO III. Actuaciones para el mantenimiento y restablecimiento de la seguridad ciudadana . . . 397
Sección 1.ª Potestades generales de policía de seguridad . . . 397
Sección 2.ª Mantenimiento y restablecimiento de la seguridad ciudadana en reuniones y manifestaciones . . . 399
CAPÍTULO IV. Potestades especiales de policía administrativa de seguridad . . . 400
CAPÍTULO V. Régimen sancionador . . . 401
Sección 1.ª Sujetos responsables, órganos competentes y reglas generales sobre las infracciones y la aplicación de las sanciones . . . 401
Sección 2.ª Infracciones y sanciones . . . 403
Sección 3.ª Procedimiento sancionador . . . 409
Disposiciones adicionales . . . 412
Disposiciones transitorias . . . 413
Disposiciones derogatorias . . . 413
Disposiciones finales . . . 413

§ 27. Ley 5/2014, de 4 de abril, de Seguridad Privada . . . 416

Preámbulo . . . 416
TÍTULO PRELIMINAR. Disposiciones generales . . . 422
CAPÍTULO I. Disposiciones comunes . . . 422
CAPÍTULO II. Competencias de la Administración General del Estado y de las comunidades autónomas . . . 427
TÍTULO I. Coordinación . . . 429
TÍTULO II. Empresas de seguridad privada y despachos de detectives privados . . . 430
CAPÍTULO I. Empresas de seguridad privada . . . 430
CAPÍTULO II. Despachos de detectives privados . . . 434
TÍTULO III. Personal de seguridad privada . . . 435
CAPÍTULO I. Disposiciones comunes . . . 435
CAPÍTULO II. Funciones de seguridad privada . . . 439

TÍTULO IV. Servicios y medidas de seguridad . . . 442
CAPÍTULO I. Disposiciones comunes . . . 442
CAPÍTULO II. Servicios de las empresas de seguridad privada . . . 443
CAPÍTULO III. Servicios de los despachos de detectives privados . . . 446
CAPÍTULO IV. Medidas de seguridad privada . . . 447
TÍTULO V. Control administrativo . . . 449
TÍTULO VI. Régimen sancionador . . . 451
CAPÍTULO I. Infracciones . . . 451
CAPÍTULO II. Sanciones . . . 457
CAPÍTULO III. Procedimiento . . . 459
Disposiciones adicionales . . . 460
Disposiciones transitorias . . . 461
Disposiciones derogatorias . . . 462
Disposiciones finales . . . 462

§ 28. Real Decreto 2364/1994, de 9 de diciembre, por el que se aprueba el Reglamento de Seguridad Privada . . . 464

Preámbulo . . . 464
Artículos . . . 465
Disposiciones adicionales . . . 465
Disposiciones transitorias . . . 467
Disposiciones derogatorias . . . 471
Disposiciones finales . . . 471
REGLAMENTO DE SEGURIDAD PRIVADA . . . 472
TITULO I. Empresas de Seguridad . . . 472
CAPITULO I. Inscripción y autorización . . . 472
CAPITULO II. Modificaciones de inscripción y cancelación . . . 476
Sección 1.ª Modificaciones de inscripción . . . 476
Sección 2.ª Cancelación . . . 476
CAPITULO III. Funcionamiento . . . 477
Sección 1.ª Disposiciones comunes . . . 477
Sección 2.ª Empresas inscritas para actividades de vigilancia, protección de personas y bienes, depósito, transporte y distribución de objetos valiosos, explosivos u objetos peligrosos . . . 480
Sección 3.ª Protección de personas . . . 481
Sección 4.ª Depósito y custodia de objetos valiosos o peligrosos y explosivos . . . 482
Sección 5.ª Transporte y distribución de objetos valiosos o peligrosos y explosivos . . . 483
Sección 6.ª Instalación y mantenimiento de aparatos, dispositivos y sistemas de seguridad . . . 484
Sección 7.ª Centrales de alarmas . . . 486
TITULO II. Personal de seguridad . . . 488
CAPITULO I. Habilitación y formación . . . 488
Sección 1.ª Requisitos . . . 488
Sección 2.ª Formación . . . 490
Sección 3.ª Procedimiento de habilitación . . . 491
Sección 4.ª Pérdida de la habilitación . . . 492
CAPITULO II. Funciones, deberes y responsabilidades . . . 492
Sección 1.ª Disposiciones comunes . . . 492
Sección 2.ª Vigilantes de seguridad . . . 493
Sección 3.ª Escoltas privados . . . 499
Sección 4.ª Guardas particulares del campo . . . 499
Sección 5.ª Jefes y directores de seguridad . . . 500
Sección 6.ª Detectives privados . . . 502
TITULO III. Medidas de seguridad . . . 504
CAPITULO I. Medidas de seguridad en general . . . 504
Sección 1.ª Disposiciones comunes . . . 504
Sección 2.ª Servicios y sistemas de seguridad . . . 504
CAPITULO II. Medidas de seguridad específicas . . . 506
Sección 1.ª Bancos, cajas de ahorro y demás entidades de credito . . . 506
Sección 2.ª Joyerías, platerías, galerías de arte y tiendas de antigüedades . . . 509
Sección 3.ª Estaciones de servicio y unidades de suministro de combustibles y carburantes . . . 510
Sección 4.ª Oficinas de farmacia, Administraciones de Lotería, Despachos de Apuestas Mutuas y establecimientos de juego . . . 511
Sección 5.ª Mantenimiento de las medidas de seguridad . . . 512
CAPITULO III. Apertura de establecimientos u oficinas obligados a disponer de medidas de seguridad . . . 512
TITULO IV. Control e inspección . . . 513

CAPITULO I. Información y control . . . 513
CAPITULO II. Inspección . . . 515
CAPITULO III. Medidas cautelares . . . 516
TITULO V. Régimen sancionador . . . 516
CAPITULO I. Cuadro de infracciones . . . 516
Sección 1.ª Empresas de seguridad . . . 516
Sección 2.ª Personal de seguridad privada . . . 520
Sección 3.ª Usuarios de los servicios de seguridad . . . 522
Sección 4.ª Infracciones al régimen de medidas de seguridad . . . 523
CAPITULO II. Procedimiento . . . 524
ANEXO. Requisitos específicos de las empresas de seguridad, según las distintas clases de actividad . . . 527

EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD

§ 29. Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. [Inclusión parcial] . . . 533

[. . .]

Disposiciones adicionales . . . 533

§ 30. Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional . 535

Preámbulo . . . 535
Artículos . . . 536
Disposiciones derogatorias . . . 537
Disposiciones finales . . . 537

§ 31. Real Decreto 521/2020, de 19 de mayo, por el que se establece la organización básica de las Fuerzas Armadas. [Inclusión parcial] . . . 538

[. . .]

TÍTULO II. Estructura operativa de las Fuerzas Armadas . . . 538

[. . .]

CAPÍTULO II. El Estado Mayor de la Defensa . . . 538
Artículo 9. El Estado Mayor de la Defensa . . . 538

[. . .]

CAPÍTULO IV. Los órganos de la estructura del Estado Mayor de la Defensa . . . 539

[. . .]

Artículo 13. El Mando Conjunto del Ciberespacio . . . 539

[. . .]

§ 32. Orden DEF/710/2020, de 27 de julio, por la que se desarrolla la organización básica del Estado Mayor de la Defensa. [Inclusión parcial] . . . 540

Disposiciones adicionales . . . 540
ORGANIZACIÓN DEL ESTADO MAYOR DE LA DEFENSA . . . 540

TELECOMUNICACIONES Y USUARIOS

§ 33. Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico . . . 542

Preámbulo . . . 542
TÍTULO I. Disposiciones generales . . . 545
CAPÍTULO I. Objeto . . . 545

CAPÍTULO II. Ámbito de aplicación . . . 545
TÍTULO II. Prestación de servicios de la sociedad de la información . . . 547
CAPÍTULO I. Principio de libre prestación de servicios . . . 547
CAPÍTULO II. Obligaciones y régimen de responsabilidad de los prestadores de servicios de la sociedad de la información . . . 548
Sección 1.ª Obligaciones . . . 548
Sección 2.ª Régimen de responsabilidad . . . 551
CAPÍTULO III. Códigos de conducta . . . 553
TÍTULO III. Comunicaciones comerciales por vía electrónica . . . 553
TÍTULO IV. Contratación por vía electrónica . . . 555
TÍTULO V. Solución judicial y extrajudicial de conflictos . . . 557
CAPÍTULO I. Acción de cesación . . . 557
CAPÍTULO II. Solución extrajudicial de conflictos . . . 557
TÍTULO VI. Información y control . . . 558
TÍTULO VII. Infracciones y sanciones . . . 560
Disposiciones adicionales . . . 565
Disposiciones transitorias . . . 570
Disposiciones finales . . . 570
ANEXO. Definiciones . . . 573

§ 34. Real Decreto 381/2015, de 14 de mayo, por el que se establecen medidas contra el tráfico no permitido y el tráfico irregular con fines fraudulentos en comunicaciones electrónicas . . . 575

Preámbulo . . . 575
Artículos . . . 577
Disposiciones adicionales . . . 581
Disposiciones transitorias . . . 582
Disposiciones finales . . . 582

§ 35. Orden TDF/149/2025, de 12 de febrero, por la que se establecen medidas para combatir las estafas de suplantación de identidad a través de llamadas telefónicas y mensajes de texto fraudulentos y para garantizar la identificación de la numeración utilizada para la prestación de servicios de atención al cliente y realización de llamadas comerciales no solicitadas . . . 584

Preámbulo . . . 584
CAPÍTULO I. Disposiciones generales . . . 586
CAPÍTULO II. Medidas para evitar que progresen las comunicaciones con manipulación del identificador de línea llamante . . . 588
CAPÍTULO III. Medidas para evitar fraudes en el ámbito de los servicios de mensajería . . . 589
CAPÍTULO IV. Medidas para garantizar la correcta identificación de la numeración utilizada para la prestación de servicios de atención a clientes y la realización de llamadas comerciales no solicitadas . . . 590
Disposiciones adicionales . . . 591
Disposiciones finales . . . 591

§ 36. Real Decreto 1163/2005, de 30 de septiembre, por el que se regula el distintivo público de confianza en los servicios de la sociedad de la información y de comercio electrónico, así como los requisitos y el procedimiento de concesión . . . 592

Preámbulo . . . 592
CAPÍTULO I. Disposiciones generales . . . 593
CAPÍTULO II. Requisitos de los códigos de conducta . . . 594
CAPÍTULO III. Obligaciones de las entidades promotoras . . . 596
CAPÍTULO IV. Concesión y retirada del distintivo . . . 596
CAPÍTULO V. Actuaciones de control . . . 598
Disposiciones transitorias . . . 598
Disposiciones derogatorias . . . 599
Disposiciones finales . . . 599
ANEXO . . . 599

§ 37. Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos . . . 601

Preámbulo . . . 601
Artículos . . . 606

Disposiciones transitorias . . . 606
Disposiciones derogatorias . . . 607
Disposiciones finales . . . 607
REGLAMENTO DE ACTUACIÓN Y FUNCIONAMIENTO DEL SECTOR PÚBLICO POR MEDIOS ELECTRÓNICOS . . . 614
TÍTULO PRELIMINAR. Disposiciones generales . . . 614
TÍTULO I. Portales de internet, Punto de Acceso General electrónico y sedes electrónicas . . . 616
TÍTULO II. Procedimiento administrativo por medios electrónicos . . . 620
CAPÍTULO I. Disposiciones generales . . . 620
CAPÍTULO II. De la identificación y autenticación de las Administraciones Públicas y las personas interesadas . . . 621
Sección 1.ª Disposiciones comunes a la identificación y autenticación y condiciones de interoperabilidad. . . 621
Sección 2.ª Identificación electrónica de las administraciones públicas y autenticación del ejercicio de su competencia . . . 622
Sección 3.ª Identificación y firma de las personas interesadas . . . 626
Sección 4.ª Acreditación de la representación de las personas interesadas . . . 629
CAPÍTULO III. Registros, comunicaciones y notificaciones electrónicas . . . 632
Sección 1.ª Registros electrónicos . . . 632
Sección 2.ª Comunicaciones y notificaciones electrónicas . . . 634
TÍTULO III. Expediente administrativo electrónico . . . 638
CAPÍTULO I. Documento administrativo electrónico y copias . . . 638
CAPÍTULO II. Archivo electrónico de documentos . . . 640
TÍTULO IV. De las relaciones y colaboración entre las Administraciones Públicas para el funcionamiento del sector público por medios electrónicos . . . 641
CAPÍTULO I. Colaboración entre las Administraciones Públicas para la actuación administrativa por medios electrónicos . . . 641
CAPÍTULO II. Transferencia y uso compartido de tecnologías entre Administraciones Públicas . . . 644
Disposiciones adicionales . . . 646
ANEXO. Definiciones . . . 649

§ 38. Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza . . . 653

Preámbulo . . . 653
TÍTULO I. Disposiciones generales . . . 657
TÍTULO II. Certificados electrónicos . . . 658
TÍTULO III. Obligaciones y responsabilidad de los prestadores de servicios electrónicos de confianza . . . 660
TÍTULO IV. Supervisión y control . . . 662
TÍTULO V. Infracciones y sanciones . . . 664
Disposiciones adicionales . . . 666
Disposiciones transitorias . . . 667
Disposiciones derogatorias . . . 667
Disposiciones finales . . . 667

§ 39. Ley 9/2014, de 9 de mayo, General de Telecomunicaciones. [Inclusión parcial] . . . 672

[. . .]

Disposiciones adicionales . . . 672
Disposiciones transitorias . . . 674

§ 40. Ley 11/2022, de 28 de junio, General de Telecomunicaciones . . . 676

Preámbulo . . . 676
TÍTULO I. Disposiciones generales . . . 682
TÍTULO II. Suministro de redes y prestación de servicios de comunicaciones electrónicas en régimen de libre competencia . . . 686
CAPÍTULO I. Disposiciones generales . . . 686
CAPÍTULO II. Notificaciones . . . 690
CAPÍTULO III. Acceso a las redes y recursos asociados e interconexión . . . 693
CAPÍTULO IV. Regulación ex ante de los mercados . . . 694
CAPÍTULO V. Separación funcional . . . 704
CAPÍTULO VI. Resolución de conflictos . . . 706
CAPÍTULO VII. Numeración . . . 707

TÍTULO III. Obligaciones de servicio público y derechos y obligaciones de carácter público en el suministro de redes y en la prestación de servicios de comunicaciones electrónicas . . . 711
CAPÍTULO I. Obligaciones de servicio público . . . 711
Sección 1.ª Delimitación . . . 711
Sección 2.ª El servicio universal . . . 712
Sección 3.ª Otras obligaciones de servicio público . . . 716
CAPÍTULO II. Derechos de los operadores y despliegue de redes públicas de comunicaciones electrónicas . . . 716
Sección 1.ª Derechos de los operadores a la ocupación del dominio público, a ser beneficiarios en el procedimiento de expropiación forzosa y al establecimiento a su favor de servidumbres y de limitaciones a la propiedad . . . 716
Sección 2.ª Normativa de las Administraciones públicas que afecte a la instalación o explotación de redes públicas de comunicaciones electrónicas . . . 719
Sección 3.ª Acceso a infraestructuras susceptibles de alojar redes públicas de comunicaciones electrónicas y coordinación de obras civiles . . . 726
Sección 4.ª Infraestructuras comunes y redes de comunicaciones electrónicas en los edificios . . . 730
CAPÍTULO III. Salvaguardia de derechos fundamentales, secreto de las comunicaciones y protección de los datos personales y derechos y obligaciones de carácter público vinculados con las redes y servicios de comunicaciones electrónicas . . . 733
CAPÍTULO IV. Derechos de los usuarios finales . . . 739
TÍTULO IV. Equipos de telecomunicación . . . 754
TÍTULO V. Dominio público radioeléctrico . . . 758
TÍTULO VI. La administración de las telecomunicaciones . . . 771
TÍTULO VII. Tasas en materia de telecomunicaciones . . . 777
TÍTULO VIII. Inspección y régimen sancionador . . . 777
Disposiciones adicionales . . . 788
Disposiciones transitorias . . . 798
Disposiciones derogatorias . . . 800
Disposiciones finales . . . 800
ANEXO I. Tasas en materia de telecomunicaciones . . . 802
ANEXO II. Definiciones . . . 808
ANEXO III . . . 814

§ 41. Real Decreto 123/2017, de 24 de febrero, por el que se aprueba el Reglamento sobre el uso del dominio público radioeléctrico . . . 816

Preámbulo . . . 816
Artículos . . . 819
Disposiciones adicionales . . . 819
Disposiciones transitorias . . . 819
Disposiciones derogatorias . . . 821
Disposiciones finales . . . 821
REGLAMENTO SOBRE EL USO DEL DOMINIO PÚBLICO RADIOELÉCTRICO . . . 822
TÍTULO I. Disposiciones generales . . . 822
TÍTULO II. Planificación del dominio público radioeléctrico . . . 824
TÍTULO III. Uso del dominio público radioeléctrico . . . 827
CAPÍTULO I. Disposiciones comunes a los diferentes usos del dominio público radioeléctrico . . . 827
CAPÍTULO II. Estaciones radioeléctricas y su instalación y operación . . . 829
CAPÍTULO III. Uso común del dominio público radioeléctrico . . . 830
CAPÍTULO IV. Uso especial del dominio público radioeléctrico . . . 831
CAPÍTULO V. Uso privativo del dominio público radioeléctrico . . . 832
Sección 1.ª Normas generales . . . 832
Sección 2.ª Procedimientos de obtención de los títulos habilitantes para uso privativo del dominio público radioeléctrico . . . 833
Subsección 1.ª Uso privativo del dominio público radioeléctrico sin limitación del número. Procedimiento general . . . 833
Subsección 2.ª Uso privativo del dominio público radioeléctrico en una banda reservada . . . 836
Subsección 3.ª Uso privativo del dominio público radioeléctrico con limitación de número de titulares. Procedimiento de licitación . . . 836
Subsección 4.ª Uso privativo del dominio público radioeléctrico para la prestación de servicios de radiodifusión sonora y de televisión . . . 839
Subsección 5.ª De los recursos órbita-espectro . . . 839
Subsección 6.ª Uso privativo del dominio público radioeléctrico para fines experimentales y eventos de corta duración . . . 842
Sección 3.ª Instalación de estaciones radioeléctricas destinadas al uso privativo del dominio público radioeléctrico . . . 843

TÍTULO IV. Puesta en servicio de las estaciones radioeléctricas . . . 848
TÍTULO V. Servicios de radiocomunicaciones que utilizan el dominio público radioeléctrico para la defensa nacional . . . 852
TÍTULO VI. Mercado secundario del espectro . . . 853
CAPÍTULO I. Disposiciones generales . . . 853
CAPÍTULO II. Transferencia de títulos que habilitan al uso privativo del dominio público radioeléctrico . . . 856
CAPÍTULO III. Cesión de derechos de uso privativo del dominio público radioeléctrico . . . 857
CAPÍTULO IV. Mutualización de los derechos de uso del dominio público radioeléctrico . . . 859
CAPÍTULO V. Provisión de servicios mayoristas relevantes . . . 861
CAPÍTULO VI. Acaparamiento de recursos de dominio público radioeléctrico . . . 862
TÍTULO VII. Duración, modificación, extinción y revocación de los títulos habilitantes para el uso del dominio público radioeléctrico . . . 864
TÍTULO VIII. Inspección y control del dominio público radioeléctrico . . . 868
CAPÍTULO I. Inspección de telecomunicaciones . . . 868
CAPÍTULO II. Uso adecuado del dominio público radioeléctrico . . . 870
TÍTULO IX. Protección del dominio público radioeléctrico . . . 872
CAPÍTULO I. Limitaciones y servidumbres para la protección del dominio público radioeléctrico . . . 872
CAPÍTULO II. Protección activa del dominio público radioeléctrico . . . 873
ANEXO 1. Servicios con frecuencias reservadas en las bandas indicadas susceptibles de cesión a terceros de los derechos de uso del dominio público radioeléctrico . . . 875
ANEXO 2. Limitaciones y servidumbres para la protección de determinadas instalaciones radioeléctricas . . . 875

§ 42. Real Decreto 1066/2001, de 28 de septiembre, por el que se aprueba el Reglamento que establece condiciones de protección del dominio público radioeléctrico, restricciones a las emisiones radioeléctricas y medidas de protección sanitaria frente a emisiones radioeléctricas . . . 878

Preámbulo . . . 878
Artículos . . . 880
Disposiciones adicionales . . . 880
Disposiciones derogatorias . . . 880
Disposiciones finales . . . 880
REGLAMENTO QUE ESTABLECE CONDICIONES DE PROTECCIÓN DEL DOMINIO PÚBLICO RADIOELÉCTRICO, RESTRICCIONES A LAS EMISIONES RADIOELÉCTRICAS Y MEDIDAS DE PROTECCIÓN SANITARIA FRENTE A EMISIONES RADIOELÉCTRICAS . . . 881
CAPITULO I. Disposiciones generales . . . 881
CAPITULO II. Protección del dominio público radioeléctrico . . . 881
CAPITULO III. Límites de exposición para la protección sanitaria y evaluación de riesgos por emisiones radioeléctricas . . . 882
CAPITULO IV. Autorización e inspección de instalaciones radioeléctricas en relación con los límites de exposición . . . 882
CAPITULO V. Otras disposiciones . . . 882
Disposiciones transitorias . . . 883
ANEXO I. Limitaciones y servidumbres para la protección de determinadas instalaciones radioeléctricas . . . 883
ANEXO II. Límites de exposición a las emisiones radioeléctricas . . . 883

§ 43. Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones . . . 892

Preámbulo . . . 892
CAPÍTULO I. Disposiciones generales . . . 894
CAPÍTULO II. Conservación y cesión de datos . . . 896
CAPÍTULO III. Infracciones y sanciones . . . 898
Disposiciones adicionales . . . 898
Disposiciones transitorias . . . 899
Disposiciones derogatorias . . . 899
Disposiciones finales . . . 900

§ 44. Orden PRE/199/2013, de 29 de enero, por la que se define el formato de entrega de los datos conservados por los operadores de servicios de comunicaciones electrónicas o de redes públicas de comunicaciones a los agentes facultados . . . 903

Preámbulo . . . 903
Artículos . . . 904
Disposiciones transitorias . . . 906

Disposiciones finales . . . 906
ANEXOS . . . 906

§ 45. Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación . . . 907

Preámbulo . . . 907
CAPÍTULO I. Disposiciones generales . . . 910
CAPÍTULO II. Análisis de riesgos . . . 912
CAPÍTULO III. Gestión de los riesgos . . . 914
CAPÍTULO IV. Esquema Nacional de Seguridad de redes y servicios 5G . . . 919
CAPÍTULO V. Inspección y régimen sancionador . . . 922
Disposiciones adicionales . . . 923
Disposiciones transitorias . . . 923
Disposiciones finales . . . 924

§ 46. Real Decreto 443/2024, de 30 de abril, por el que se aprueba el Esquema Nacional de Seguridad de redes y servicios 5G. . . . 925

Preámbulo . . . 925
Artículos . . . 927
Disposiciones adicionales . . . 927
Disposiciones finales . . . 927
ESQUEMA NACIONAL DE SEGURIDAD DE LAS REDES Y SERVICIOS 5G . . . 928
CAPÍTULO I. Disposiciones generales . . . 928
CAPÍTULO II. Análisis y gestión de riesgos a nivel nacional . . . 932
CAPÍTULO III. Medidas específicas para garantizar la seguridad de las redes y servicios 5G . . . 933
CAPÍTULO IV. Análisis de riesgos por los sujetos obligados . . . 936
CAPÍTULO V. Gestión de los riesgos por los sujetos obligados . . . 939
CAPÍTULO VI. Otras medidas de cumplimiento en materia de la seguridad de las redes y servicios 5G . . . 945
CAPÍTULO VII. Aplicación del ENS5G . . . 948
CAPÍTULO VIII. Inspección y régimen sancionador . . . 949
ANEXO I. Elementos, infraestructuras y recursos que integran una red 5G . . . 950
ANEXO II. Análisis de riesgos a nivel nacional . . . 956
ANEXO III. Gestión de riesgos a nivel nacional . . . 967

§ 47. Real Decreto 255/2025, de 1 de abril, por el que se regula el Documento Nacional de Identidad . . . 970

Preámbulo . . . 970
CAPÍTULO I. Disposiciones generales . . . 972
CAPÍTULO II. Sobre derechos, obligaciones y órganos competentes . . . 973
CAPÍTULO III. Sobre tramitación, expedición, validez y renovación . . . 973
CAPÍTULO IV. Sobre las especificidades de la versión digital del Documento Nacional de Identidad . . . 977
CAPÍTULO V. Sobre la protección en el tratamiento de los datos personales . . . 977
Disposiciones adicionales . . . 977
Disposiciones transitorias . . . 978
Disposiciones derogatorias . . . 978
Disposiciones finales . . . 979

CIBERDELINCUENCIA

§ 48. Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. [Inclusión parcial]. . . . 981

[. . .]

LIBRO I. Disposiciones generales sobre los delitos, las personas responsables, las penas, medidas de seguridad y demás consecuencias de la infracción penal. . . . 981

[. . .]

TÍTULO II. De las personas criminalmente responsables de los delitos . . . 981

[. . .]

TÍTULO V. De la responsabilidad civil derivada de los delitos y de las costas procesales . . . 984
CAPÍTULO I. De la responsabilidad civil y su extensión . . . 984
CAPÍTULO II. De las personas civilmente responsables . . . 985

[. . .]

CAPÍTULO II. De las amenazas . . . 987
CAPÍTULO III. De las coacciones . . . 988

[. . .]

CAPÍTULO IV. De los delitos de exhibicionismo y provocación sexual . . . 990
CAPÍTULO V. De los delitos relativos a la prostitución y a la explotación sexual y corrupción de menores . . . 990
CAPÍTULO VI. Disposiciones comunes a los capítulos anteriores . . . 993

[. . .]

TÍTULO X. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio . . . 994
CAPÍTULO I. Del descubrimiento y revelación de secretos . . . 994

[. . .]

TÍTULO XI. Delitos contra el honor . . . 996
CAPÍTULO I. De la calumnia . . . 996
CAPÍTULO II. De la injuria . . . 996
CAPÍTULO III. Disposiciones generales . . . 997

[. . .]

Sección 1.ª De las estafas . . . 998

[. . .]

CAPÍTULO X. Disposiciones comunes a los capítulos anteriores . . . 1002
CAPÍTULO XI. De los delitos relativos a la propiedad intelectual e industrial, al mercado y a los consumidores . . . 1002
Sección 1.ª De los delitos relativos a la propiedad intelectual . . . 1002
Sección 2.ª De los delitos relativos a la propiedad industrial . . . 1004
Sección 3.ª De los delitos relativos al mercado y a los consumidores . . . 1005
Sección 4.ª Delitos de corrupción en los negocios . . . 1009

[. . .]

TÍTULO XVI bis. De los delitos contra los animales . . . 1010

[. . .]

TÍTULO XVIII. De las falsedades . . . 1012

[. . .]

CAPÍTULO IV. De la usurpación del estado civil . . . 1012

[. . .]

CAPÍTULO III. Del descubrimiento y revelación de secretos e informaciones relativas a la Defensa Nacional 1012

[. . .]

§ 49. Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores. [Inclusión parcial] . . . 1014

TÍTULO PRELIMINAR . . . 1014
TÍTULO I. Del ámbito de aplicación de la Ley . . . 1014
TÍTULO II. De las medidas . . . 1017

[. . .]

§ 50. Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal. [Inclusión parcial] . . . 1023

Artículos . . . 1023

[. . .]

LIBRO II. Del sumario . . . 1024
TÍTULO I. De la denuncia . . . 1024
TÍTULO II. De la querella . . . 1027
TÍTULO III. De la Policía judicial . . . 1029

[. . .]

TÍTULO V. De la comprobación del delito y averiguación del delincuente . . . 1034

[. . .]

Capítulo II. Del cuerpo del delito . . . 1034
Capítulo II bis. De la destrucción y la realización anticipada de los efectos judiciales . . . 1036
Capítulo III. De la identidad del delincuente y de sus circunstancias personales . . . 1038

[. . .]

Capítulo VII. Del informe pericial . . . 1041

[. . .]

TÍTULO VIII. De las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución . . . 1045
CAPÍTULO I. De la entrada y registro en lugar cerrado . . . 1045
CAPÍTULO II. Del registro de libros y papeles . . . 1049
CAPÍTULO III. De la detención y apertura de la correspondencia escrita y telegráfica . . . 1050
CAPÍTULO IV. Disposiciones comunes a la interceptación de las comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen, el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos . . . 1052
CAPÍTULO V. La interceptación de las comunicaciones telefónicas y telemáticas . . . 1055
Sección 1.ª Disposiciones generales . . . 1055
Sección 2.ª Incorporación al proceso de datos electrónicos de tráfico o asociados . . . 1057
Sección 3.ª Acceso a los datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad . . . 1057
CAPÍTULO VI. Captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos . . . 1058
CAPÍTULO VII. Utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización . . . 1059
CAPÍTULO VIII. Registro de dispositivos de almacenamiento masivo de información . . . 1060
CAPÍTULO IX. Registros remotos sobre equipos informáticos . . . 1061
CAPÍTULO X. Medidas de aseguramiento . . . 1062

[. . .]

TÍTULO III . . . 1062

[. . .]

Capítulo III. Del modo de practicar las pruebas durante el juicio oral . . . 1062

[. . .]

Sección 3.ª Del informe pericial . . . 1063
Sección 4.ª De la prueba documental y de la inspección ocular . . . 1063

[. . .]

TÍTULO II. Del procedimiento abreviado . . . 1063

[. . .]

Capítulo II. De las actuaciones de la Policía Judicial y del Ministerio Fiscal . . . 1063

[. . .]

TÍTULO V. Del procedimiento por delitos cometidos por medio de la imprenta, el grabado u otro medio mecánico de publicación . . . 1066

[. . .]

PROTECCIÓN DE DATOS

§ 51. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales . . . 1068

Preámbulo . . . 1068
TÍTULO I. Disposiciones generales . . . 1075
TÍTULO II. Principios de protección de datos . . . 1076
TÍTULO III. Derechos de las personas . . . 1078
CAPÍTULO I. Transparencia e información . . . 1078
CAPÍTULO II. Ejercicio de los derechos . . . 1079
TÍTULO IV. Disposiciones aplicables a tratamientos concretos . . . 1080
TÍTULO V. Responsable y encargado del tratamiento . . . 1084
CAPÍTULO I. Disposiciones generales. Medidas de responsabilidad activa . . . 1084
CAPÍTULO II. Encargado del tratamiento . . . 1086
CAPÍTULO III. Delegado de protección de datos . . . 1087
CAPÍTULO IV. Códigos de conducta y certificación . . . 1089
TÍTULO VI. Transferencias internacionales de datos . . . 1090
TÍTULO VII. Autoridades de protección de datos . . . 1091
CAPÍTULO I. La Agencia Española de Protección de Datos . . . 1091
Sección 1.ª Disposiciones generales . . . 1091
Sección 2.ª Potestades de investigación y planes de auditoría preventiva . . . 1095
Sección 3.ª Otras potestades de la Agencia Española de Protección de Datos . . . 1097
CAPÍTULO II. Autoridades autonómicas de protección de datos . . . 1098
Sección 1.ª Disposiciones generales . . . 1098
Sección 2.ª Coordinación en el marco de los procedimientos establecidos en el Reglamento (UE) 2016/679 . . . 1099
TÍTULO VIII. Procedimientos en caso de posible vulneración de la normativa de protección de datos . . . 1099
TÍTULO IX. Régimen sancionador . . . 1103
TÍTULO X. Garantía de los derechos digitales . . . 1109
Disposiciones adicionales . . . 1115
Disposiciones transitorias . . . 1121
Disposiciones derogatorias . . . 1122
Disposiciones finales . . . 1122

§ 52. Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal . . . 1130

Preámbulo . . . 1130
Artículos . . . 1132
Disposiciones transitorias . . . 1132
Disposiciones derogatorias . . . 1133
Disposiciones finales . . . 1134
REGLAMENTO DE DESARROLLO DE LA LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE, DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL . . . 1134
TÍTULO I. Disposiciones generales . . . 1134
TÍTULO II. Principios de protección de datos . . . 1138
CAPÍTULO I. Calidad de los datos . . . 1138
CAPÍTULO II. Consentimiento para el tratamiento de los datos y deber de información . . . 1140
Sección 1.ª Obtención del consentimiento del afectado . . . 1140
Sección 2.ª Deber de información al interesado . . . 1142
CAPÍTULO III. Encargado del tratamiento . . . 1142
TÍTULO III. Derechos de acceso, rectificación, cancelación y oposición . . . 1143
CAPÍTULO I. Disposiciones generales . . . 1143
CAPÍTULO II. Derecho de acceso . . . 1145
CAPÍTULO III. Derechos de rectificación y cancelación . . . 1147
CAPÍTULO IV. Derecho de oposición . . . 1147
TÍTULO IV. Disposiciones aplicables a determinados ficheros de titularidad privada . . . 1148
CAPÍTULO I. Ficheros de información sobre solvencia patrimonial y crédito . . . 1148
Sección 1.ª Disposiciones generales . . . 1148
Sección 2.ª Tratamiento de datos relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés . . . 1149
CAPÍTULO II. Tratamientos para actividades de publicidad y prospección comercial . . . 1151

TÍTULO V. Obligaciones previas al tratamiento de los datos . . . 1154
CAPÍTULO I. Creación, modificación o supresión de ficheros de titularidad pública. . . . 1154
CAPÍTULO II. Notificación e inscripción de los ficheros de titularidad pública o privada . . . 1155
TÍTULO VI. Transferencias internacionales de datos. . . . 1158
CAPÍTULO I. Disposiciones generales . . . 1158
CAPÍTULO II. Transferencias a estados que proporcionen un nivel adecuado de protección. . . . 1158
CAPÍTULO III. Transferencias a Estados que no proporcionen un nivel adecuado de protección . . . 1159
TÍTULO VII. Códigos tipo . . . 1160
TÍTULO VIII. De las medidas de seguridad en el tratamiento de datos de carácter personal. . . . 1163
CAPÍTULO I. Disposiciones generales . . . 1163
CAPÍTULO II. Del documento de seguridad . . . 1165
CAPÍTULO III. Medidas de seguridad aplicables a ficheros y tratamientos automatizados . . . 1166
Sección 1.ª Medidas de seguridad de nivel básico. . . . 1166
Sección 2.ª Medidas de seguridad de nivel medio . . . 1168
Sección 3.ª Medidas de seguridad de nivel alto. . . . 1169
CAPÍTULO IV. Medidas de seguridad aplicables a los ficheros y tratamientos no automatizados . . . 1170
Sección 1.ª Medidas de seguridad de nivel básico. . . . 1170
Sección 2.ª Medidas de seguridad de nivel medio . . . 1171
Sección 3.ª Medidas de seguridad de nivel alto. . . . 1171
TÍTULO IX. Procedimientos tramitados por la Agencia Española de Protección de Datos . . . 1172
CAPÍTULO I. Disposiciones generales . . . 1172
CAPÍTULO II. Procedimiento de tutela de los derechos de acceso, rectificación, cancelación y oposición . . . 1172
CAPÍTULO III. Procedimientos relativos al ejercicio de la potestad sancionadora . . . 1173
Sección 1.ª Disposiciones generales . . . 1173
Sección 2.ª Actuaciones previas . . . 1174
Sección 3.ª Procedimiento sancionador . . . 1175
Sección 4.ª Procedimiento de declaración de infracción de la Ley Orgánica 15/1999, de 13 de diciembre, por las administraciones públicas. . . . 1175
CAPÍTULO IV. Procedimientos relacionados con la inscripción o cancelación de ficheros. . . . 1176
Sección 1.ª Procedimiento de inscripción de la creación, modificación o supresión de ficheros. . . . 1176
Sección 2.ª Procedimiento de cancelación de oficio de ficheros inscritos . . . 1177
CAPÍTULO V. Procedimientos relacionados con las transferencias internacionales de datos. . . . 1177
Sección 1.ª Procedimiento de autorización de transferencias internacionales de datos. . . . 1177
Sección 2.ª Procedimiento de suspensión temporal de transferencias internacionales de datos . . . 1178
CAPÍTULO VI. Procedimiento de inscripción de códigos tipo. . . . 1179
CAPÍTULO VII. Otros procedimientos tramitados por la agencia española de protección de datos . . . 1180
Sección 1.ª Procedimiento de exención del deber de información al interesado . . . 1180
Sección 2.ª Procedimiento para la autorización de conservación de datos para fines históricos, estadísticos o científicos . . . 1181
Disposiciones adicionales . . . 1182

§ 53. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) . . . 1183

Preámbulo . . . 1183
CAPÍTULO I. Disposiciones generales . . . 1218
CAPÍTULO II. Principios . . . 1222
CAPÍTULO III. Derechos del interesado. . . . 1226
Sección 1. Transparencia y modalidades . . . 1226
Sección 2. Información y acceso a los datos personales . . . 1227
Sección 3. Rectificación y supresión . . . 1229
Sección 4. Derecho de oposición y decisiones individuales automatizadas . . . 1231
Sección 5. Limitaciones . . . 1232
CAPÍTULO IV. Responsable del tratamiento y encargado del tratamiento . . . 1233
Sección 1. Obligaciones generales . . . 1233
Sección 2. Seguridad de los datos personales . . . 1237
Sección 3. Evaluación de impacto relativa a la protección de datos y consulta previa . . . 1238
Sección 4. Delegado de protección de datos . . . 1240
Sección 5. Códigos de conducta y certificación . . . 1242
CAPÍTULO V. Transferencias de datos personales a terceros países u organizaciones internacionales . . . 1246
CAPÍTULO VI. Autoridades de control independientes . . . 1251
Sección 1. Independencia. . . . 1251
Sección 2. Competencia, funciones y poderes . . . 1252

CAPÍTULO VII. Cooperación y coherencia . . . 1256
Sección 1. Cooperación y coherencia . . . 1256
Sección 2. Coherencia . . . 1259
Sección 3. Comité europeo de protección de datos . . . 1261
CAPÍTULO VIII. Recursos, responsabilidad y sanciones . . . 1265
CAPÍTULO IX. Disposiciones relativas a situaciones específicas de tratamiento . . . 1268
CAPÍTULO X. Actos delegados y actos de ejecución . . . 1270
CAPÍTULO XI. Disposiciones finales . . . 1271

§ 54. Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. [Inclusión parcial] . . . 1273

Preámbulo . . . 1273
CAPÍTULO I. Disposiciones generales . . . 1280
CAPÍTULO II. Principios, licitud del tratamiento y videovigilancia . . . 1282
Sección 1.ª Principios y licitud del tratamiento . . . 1282
Sección 2.ª Tratamiento de datos personales en el ámbito de la videovigilancia por Fuerzas y Cuerpos de Seguridad . . . 1286
CAPÍTULO III. Derechos de las personas . . . 1288
Sección 1.ª Régimen general . . . 1288
Sección 2.ª Régimen especial . . . 1291
CAPÍTULO IV. Responsable y encargado de tratamiento . . . 1291
Sección 1.ª Obligaciones generales . . . 1291
Sección 2.ª Seguridad de los datos personales . . . 1295
Sección 3.ª Delegado de protección de datos . . . 1297
CAPÍTULO V. Transferencias de datos personales a terceros países que no sean miembros de la Unión Europea o a organizaciones internacionales . . . 1298
CAPÍTULO VI. Autoridades de Protección de Datos Independientes . . . 1300
CAPÍTULO VII. Reclamaciones . . . 1302
CAPÍTULO VIII. Régimen sancionador . . . 1304
Disposiciones adicionales . . . 1308
Disposiciones transitorias . . . 1309
Disposiciones derogatorias . . . 1309
Disposiciones finales . . . 1309

RELACIONES CON LA ADMINISTRACIÓN

§ 55. Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. [Inclusión parcial] . . . 1311

[. . .]

TÍTULO II. De la actividad de las Administraciones Públicas . . . 1311
CAPÍTULO I. Normas generales de actuación . . . 1311
CAPÍTULO II. Términos y plazos . . . 1315
TÍTULO III. De los actos administrativos . . . 1317

[. . .]

CAPÍTULO II. Eficacia de los actos . . . 1317

[. . .]

TÍTULO IV. De las disposiciones sobre el procedimiento administrativo común . . . 1317

[. . .]

CAPÍTULO III. Ordenación del procedimiento . . . 1317

[. . .]

Disposiciones adicionales . . . 1318

§ 56. Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. [Inclusión parcial] . . . 1320

TÍTULO PRELIMINAR. Disposiciones generales, principios de actuación y funcionamiento del sector público . . . 1320

CAPÍTULO I. Disposiciones generales 1320
CAPÍTULO II. De los órganos de las Administraciones Públicas 1321

[. . .]

Sección 2.ª Competencia 1321

[. . .]

CAPÍTULO V. Funcionamiento electrónico del sector público 1322

[. . .]

TÍTULO III. Relaciones interadministrativas 1324

[. . .]

CAPÍTULO IV. Relaciones electrónicas entre las Administraciones 1324
Disposiciones adicionales 1326

§ 1

Nota del autor

Última modificación: 15 de noviembre de 2021

Promovida por el Consejo de Seguridad Nacional, en el año 2013 se publicó la Estrategia de Seguridad Nacional, que contempla la ciberseguridad dentro de sus doce ámbitos de actuación. El propósito de este documento es el de fijar las directrices generales del uso seguro del ciberespacio a través del impulso de una visión integradora que garantice la seguridad y el progreso de España. Tal objetivo debía alcanzarse a través de la adecuada coordinación y cooperación entre todas las Administraciones Públicas, pero también entre aquellas con el sector privado y con los ciudadanos.

La Estrategia persigue lograr la seguridad del ciberespacio a través del desarrollo y aplicación de una política de ciberseguridad nacional, lo que exige contar con un adecuado marco normativo que proporcione una mayor confianza en el uso de las TIC. Dicho fin no sólo tienen que ver la implantación de un marco nacional de políticas públicas, procedimientos y normas técnicas, sino que alcanza a una necesidad de mantener actualizado el ordenamiento jurídico en una materia como la que ahora nos ocupa.

En particular, el Objetivo III de la citada Estrategia ya se refiere a la necesidad de armonizar las legislaciones nacionales a través del desarrollo y mantenimiento de una regulación sólida y eficaz. Por su parte, el Objetivo IV llama a desarrollar una gestión eficaz de los riesgos derivados del ciberespacio sobre la que poder edificar una sólida cultura de ciberseguridad, para lo cual se requiere lograr que los usuarios tengan una especial sensibilización en cuanto al conocimiento de las herramientas para la protección de su información, sistemas y servicios.

Alineada con la citada Estrategia de Seguridad Nacional de 2013, ese mismo año se publica la Estrategia de Ciberseguridad Nacional, la cual se articula a través de una serie de líneas de acción. A los efectos que aquí nos interesan, las líneas de acción 4 y 6 incluyen una serie de referencias con especial incidencia en los aspectos legales de la ciberseguridad. En particular, la línea de acción 4 contempla una serie de medidas destinadas a integrar en el marco legal español las soluciones a los nuevos problemas relacionados con la ciberseguridad en el ámbito penal, y asegurar a los profesionales del Derecho el acceso a la información y a los recursos que les proporcionen el nivel necesario de conocimientos en el ámbito judicial para la mejor aplicación del marco legal y técnico asociado.

A estos efectos, el Instituto Nacional de Ciberseguridad de España (INCIBE), organismo dependiente de la Secretaría de Estado para el Avance Digital del Ministerio de Economía y Empresa, dentro de las funciones que tienen encomendadas para el desarrollo y aplicación de las políticas de ciberseguridad, propone compilar en este documento toda la legislación española que afecte a la ciberseguridad, al objeto de contribuir a mejorar el conocimiento y facilitar la aplicación de una normativa que afecta a una materia tan importante, pero a su vez tan cambiante.

El carácter transversal de la ciberseguridad hace innecesaria la inclusión en este compendio de todas las normas de naturaleza general o, en otras palabras, no exclusivas de esta materia (por citar algunas, la reciente aprobación de la normativa de protección de datos –Reglamento y Directiva- o las últimas modificaciones del código penal en materia de ciberdelitos), que sí son de referencia necesaria en otros códigos normativos ya existentes. De ahí, en ocasiones, su mera referencia en la presente obra.

Sí merece destacar que en fecha 19 de julio de 2016 se publicó en el DOUE la Directiva del Parlamento Europeo y del Consejo relativa a medidas para garantizar un elevado nivel común de seguridad de las redes y de la información en la Unión (comúnmente conocida como "Directiva NIS"), que se trata de un documento imprescindible para conocer las nuevas obligaciones exigidas en el campo de la ciberseguridad, y las competencias otorgadas a algunos de los agentes que intervienen en ella –caso de los CERT- y cuya transposición se realizó a través del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

La Administración Pública no ha resultado ajena a las nuevas necesidades derivadas de la protección de los sistemas y redes de información. Fruto de ello, mediante Resolución de 27 de diciembre de 2018, de la Subsecretaría, se publicó en el Boletín Oficial del Estado de 1 de enero de 2019, el Convenio en materia de ciberseguridad entre el Ministerio de Política Territorial y Función Pública y el Centro Nacional de Inteligencia, mediante el cual se constituirá un Centro de Operaciones de Ciberseguridad (SOC) para el Ministerio de Política Territorial y Función Pública, que operará como una extensión del Centro de Operaciones de Ciberseguridad de la Administración General del Estado (SOC de la AGE) tendiendo de manera progresiva a unificar y converger las diferentes actuaciones de seguridad que se proporcionen.

En definitiva, a través de este compendio se pretende poner a disposición de todos los profesionales una herramienta donde se puedan encontrar, actualizadas, las normas que afecten directamente a la ciberseguridad, y facilitar así el necesario estudio y análisis de una materia que ya resulta imprescindible para lograr una adecuada protección de empresas, instituciones y ciudadanos dentro de un estado social y democrático de derecho.

Francisco Pérez Bes

Secretario General del Instituto Nacional de Ciberseguridad de España, S.A. (INCIBE)

ANEXO

NORMATIVA NO CONSOLIDADA

I - NORMATIVA INTERNACIONAL Y COMUNITARIA

§ 1. Convenio sobre la ciberdelincuencia (Budapest) de 23 de noviembre de 2001.

https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221

§ 2. Protocolo Adicional a la Convención de Budapest del Consejo de Europa sobre persecución de los actos de racismo y xenofobia cometidos a través de internet.

https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-793

§ 3. Convención de Lanzarote del año 2007 del Consejo de Europa sobre abuso y explotación sexual de los menores y pornografía infantil.

https://www.boe.es/buscar/act.php?id=BOE-A-2010-17392

§ 4. Directiva 2011/93/UE sobre abuso, explotación sexual de los menores y pornografía infantil.

http://www.boe.es/buscar/doc.php?id=DOUE-L-2011-82637

http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32011L0093

§ 5. Directiva 2013/40/UE sobre ataques a los sistemas de información.

http://www.boe.es/buscar/doc.php?id=DOUE-L-2013-81648

http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=URISERV:l33193

§ 6. Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo de 15 de marzo de 2017 relativa a la lucha contra el terrorismo y por la que se sustituye la Decisión marco 2002/475/JAI del Consejo y se modifica la Decisión 2005/671/JAI del Consejo

http://data.europa.eu/eli/dir/2017/541/2017-03-31

§ 7. Directiva 2008/114/CE del Consejo, sobre Identificación y Designación de las Infraestructuras Críticas Europeas y la Evaluación de la Necesidad de Mejorar su Protección.

http://www.boe.es/buscar/doc.php?id=DOUE-L-2008-82589

http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:jl0013

§ 8. Directiva 2002/77/CE de la Comisión, de 16 de septiembre de 2002, relativa a la competencia en los mercados de redes y servicios de comunicaciones electrónicas.

http://www.boe.es/buscar/doc.php?id=DOUE-L-2002-81623

http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32002L0077

§ 9. Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas.

http://www.boe.es/buscar/doc.php?id=DOUE-L-2002-81371

http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=URISERV:l24120

§ 10. Directiva 2002/22/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas.

http://www.boe.es/buscar/doc.php?id=DOUE-L-2002-80701

http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=URISERV:l24108h

§ 11. Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2018, por la que se establece el Código Europeo de las Comunicaciones Electrónicas (versión refundida)Texto pertinente a efectos del EEE.

http://data.europa.eu/eli/dir/2018/1972/2018-12-17

§ 12. Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión

http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.SPA

§ 13. Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior.

http://www.boe.es/buscar/doc.php?id=DOUE-L-2000-81295

http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32000L0031

§ 14. Convenio 108 del Consejo de Europa sobre Protección de Datos de carácter personal.

https://www.boe.es/buscar/doc.php?id=BOE-A-1985-23447

§ 15. REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32016R0679

§ 16. REGLAMENTO (UE) Nº 611/2013 DE LA COMISION, de 24 de junio de 2013, relativo a las medidas aplicables a la notificación de casos de violación de datos personales en el marco de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo sobre la privacidad y las comunicaciones electrónicas

http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32013R0611

§ 17. Reglamento (UE) nº 526/2013 del Parlamento Europeo y del Consejo, de 21de mayo de 2013, relativo a la Agencia de Seguridad de las Redes de la Información de la Unión Europea (ENISA) y por el que se deroga el Reglamento (CE) nº460/2004.

http://www.boe.es/buscar/doc.php?id=DOUE-L-2013-81184

§ 18. Reglamento (UE) nº 513/2014 del Parlamento Europeo y del Consejo, de 16 de abril de 2014, por el que se establece, como parte del Fondo de Seguridad Interior, el instrumento de apoyo financiero a la cooperación policial, la prevención y la lucha contra la delincuencia, y la gestión de crisis y por el que se deroga la Decisión 2007/125/JAI del Consejo.

http://www.boe.es/buscar/doc.php?id=DOUE-L-2014-81034

http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32014R0513

§ 19. Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre ENISA (Agencia de la Unión Europea para la Ciberseguridad) y sobre la certificación de la ciberseguridad de la tecnología de la información y las comunicaciones y por el que se deroga el Reglamento (UE) no 526/2013 (Ley de ciberseguridad)

https://eur-lex.europa.eu/eli/reg/2019/881/oj

https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:OJ.L_.2019.151.01.0015.01.SPA

§ 20. Reglamento (UE) nº 230/2014 del Parlamento Europeo y del Consejo, de 11 de marzo de 2014, por el que se establece un instrumento en pro de la estabilidad y la paz.

http://www.boe.es/buscar/doc.php?id=DOUE-L-2014-80479

§ 21. Carta de Naciones Unidas.

https://www.boe.es/diario_boe/txt.php?id=BOE-A-1990-27553

§ 22. Recomendación (UE) 2017/1584 de la Comisión, de 13 de septiembre de 2017, sobre la respuesta coordinada a los incidentes y crisis de ciberseguridad a gran escala

http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:OJ.L_.2017.239.01.0036.01.SPA

II.- NORMATIVA NACIONAL

NORMATIVA DE SEGURIDAD NACIONAL

§ 1. Estrategia de Seguridad Nacional: http://www.lamoncloa.gob.es/documents/seguridad_1406connavegacionfinalaccesiblebpdf.pdf

§ 2. Estrategia de Ciberseguridad Nacional: http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf

§ 3. Resolución de 27 de diciembre de 2018, de la Subsecretaría, por la que se publica el Convenio en materia de ciberseguridad entre el Ministerio de Política Territorial y Función

Pública y el Centro Nacional de Inteligencia: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2019-42

§ 2

Constitución Española. [Inclusión parcial]

Cortes Generales
«BOE» núm. 311, de 29 de diciembre de 1978
Última modificación: 17 de febrero de 2024
Referencia: BOE-A-1978-31229

[. . .]

TÍTULO I

De los derechos y deberes fundamentales

[. . .]

CAPÍTULO SEGUNDO

Derechos y libertades

[. . .]

Sección 1.ª De los derechos fundamentales y de las libertades públicas

[. . .]

Artículo 17.

1. Toda persona tiene derecho a la libertad y a la seguridad. Nadie puede ser privado de su libertad, sino con la observancia de lo establecido en este artículo y en los casos y en la forma previstos en la ley.

2. La detención preventiva no podrá durar más del tiempo estrictamente necesario para la realización de las averiguaciones tendentes al esclarecimiento de los hechos, y, en todo caso, en el plazo máximo de setenta y dos horas, el detenido deberá ser puesto en libertad o a disposición de la autoridad judicial.

3. Toda persona detenida debe ser informada de forma inmediata, y de modo que le sea comprensible, de sus derechos y de las razones de su detención, no pudiendo ser obligada a declarar. Se garantiza la asistencia de abogado al detenido en las diligencias policiales y judiciales, en los términos que la ley establezca.

4. La ley regulará un procedimiento de «habeas corpus» para producir la inmediata puesta a disposición judicial de toda persona detenida ilegalmente. Asimismo, por ley se determinará el plazo máximo de duración de la prisión provisional.

Artículo 18.

1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.
2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.
3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.
4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

[. . .]

Artículo 24.

1. Todas las personas tienen derecho a obtener la tutela efectiva de los jueces y tribunales en el ejercicio de sus derechos e intereses legítimos, sin que, en ningún caso, pueda producirse indefensión.
2. Asimismo, todos tienen derecho al Juez ordinario predeterminado por la ley, a la defensa y a la asistencia de letrado, a ser informados de la acusación formulada contra ellos, a un proceso público sin dilaciones indebidas y con todas las garantías, a utilizar los medios de prueba pertinentes para su defensa, a no declarar contra sí mismos, a no confesarse culpables y a la presunción de inocencia.

La ley regulará los casos en que, por razón de parentesco o de secreto profesional, no se estará obligado a declarar sobre hechos presuntamente delictivos.

[. . .]

CAPÍTULO TERCERO

De los principios rectores de la política social y económica

Artículo 39.

1. Los poderes públicos aseguran la protección social, económica y jurídica de la familia.
2. Los poderes públicos aseguran, asimismo, la protección integral de los hijos, iguales éstos ante la ley con independencia de su filiación, y de las madres, cualquiera que sea su estado civil. La ley posibilitará la investigación de la paternidad.
3. Los padres deben prestar asistencia de todo orden a los hijos habidos dentro o fuera del matrimonio, durante su minoría de edad y en los demás casos en que legalmente proceda.
4. Los niños gozarán de la protección prevista en los acuerdos internacionales que velan por sus derechos.

[. . .]

Artículo 51.

1. Los poderes públicos garantizarán la defensa de los consumidores y usuarios, protegiendo, mediante procedimientos eficaces, la seguridad, la salud y los legítimos intereses económicos de los mismos.
2. Los poderes públicos promoverán la información y la educación de los consumidores y usuarios, fomentarán sus organizaciones y oirán a éstas en las cuestiones que puedan afectar a aquéllos, en los términos que la ley establezca.
3. En el marco de lo dispuesto por los apartados anteriores, la ley regulará el comercio interior y el régimen de autorización de productos comerciales.

[. . .]

§ 3

Ley 36/2015, de 28 de septiembre, de Seguridad Nacional

Jefatura del Estado
«BOE» núm. 233, de 29 de septiembre de 2015
Última modificación: 12 de diciembre de 2016
Referencia: BOE-A-2015-10389

FELIPE VI

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley:

PREÁMBULO

I

La seguridad constituye la base sobre la cual una sociedad puede desarrollarse, preservar su libertad y la prosperidad de sus ciudadanos, y garantizar la estabilidad y buen funcionamiento de sus instituciones.

La legislación española así lo reconoce e interpreta, y contiene instrumentos normativos que, partiendo del marco diseñado por la Constitución, regulan los aspectos fundamentales que han venido permitiendo a los poderes públicos cumplir con sus obligaciones en esta materia.

Así, las normas aplicables a los estados de alarma, excepción y sitio, a la Defensa Nacional, a las Fuerzas y Cuerpos de Seguridad, a la protección de la seguridad ciudadana, a la protección de infraestructuras críticas, a la protección civil, a la acción y el servicio exterior del Estado o a la seguridad privada, regulan, junto con la legislación penal y los tratados y compromisos internacionales en los que España es parte, distintos aspectos de la seguridad.

Esta regulación se basa en la asignación de competencias a las distintas autoridades y Administraciones Públicas, y se articula en un modelo tradicional y homologable con los países de nuestro entorno, que se ha demostrado válido hasta ahora y que ha permitido hacer frente a las necesidades de seguridad de una sociedad abierta, libre y democrática como la española.

Sin embargo, en el mundo actual, y en el entorno más previsible para el futuro, los actores y circunstancias que ponen en peligro los niveles de seguridad, se encuentran sujetos a constante mutación, y es responsabilidad de los poderes públicos dotarse de la normativa, procedimientos y recursos que le permitan responder con eficacia a estos desafíos a la seguridad.

En este contexto aparece el campo de la Seguridad Nacional como un espacio de actuación pública nuevo, enfocado a la armonización de objetivos, recursos y políticas ya existentes en materia de seguridad.

En este sentido, la Seguridad Nacional se entiende como la acción del Estado dirigida a proteger la libertad y el bienestar de sus ciudadanos, a garantizar la defensa de España y sus principios y valores constitucionales, así como a contribuir junto a nuestros socios y aliados a la seguridad internacional en cumplimiento de los compromisos asumidos; concepto que, hasta la fecha, no había sido objeto de una regulación normativa integral.

Este esfuerzo de integración reviste tanta mayor importancia cuanto que la Seguridad Nacional debe ser considerada un objetivo compartido por las diferentes Administraciones, estatal, autonómica y local, los órganos constitucionales, en especial las Cortes Generales, el sector privado y la sociedad civil, dentro de los proyectos de las organizaciones internacionales de las que formamos parte.

Por otro lado, la realidad demuestra que los desafíos para la Seguridad Nacional que afectan a la sociedad revisten en ocasiones una elevada complejidad, que desborda las fronteras de categorías tradicionales como la defensa, la seguridad pública, la acción exterior y la inteligencia, así como de otras más recientemente incorporadas a la preocupación por la seguridad, como el medio ambiente, la energía, los transportes, el ciberespacio y la estabilidad económica.

La dimensión que adquieren ciertos riesgos y amenazas, su acusada transversalidad, o la combinación de estos rasgos con su naturaleza abierta e incierta, como sucede en las situaciones de interés para la Seguridad Nacional definidas por la presente ley, son factores que indican claramente que toda respuesta que implique a los distintos agentes e instrumentos de la Seguridad Nacional se verá reforzada y resultará más eficiente si se realiza de forma coordinada.

El superior interés nacional requiere mejorar la coordinación de las diferentes Administraciones Públicas, buscando marcos de prevención y respuesta que ayuden a resolver los problemas que plantea una actuación compartimentada, organizando a diversos niveles y de manera integral, la acción coordinada de los agentes e instrumentos al servicio de la Seguridad Nacional.

Esta ley se dicta con el propósito de responder a esta demanda, que viene siendo expresada por los agentes de la Seguridad Nacional integrados en las Administraciones Públicas, por el sector privado y por la sociedad en general. No afecta a la regulación de los distintos agentes e instrumentos que ya son objeto de normas sectoriales específicas, sino que facilita su inserción armónica en el esquema de organización general, establecido por la Estrategia de Seguridad Nacional, de 31 de mayo de 2013, bajo la denominación de Sistema de Seguridad Nacional, y liderado por el Presidente del Gobierno.

II

Esta ley se estructura en cinco títulos.

En el título preliminar, además de las disposiciones relativas a su objeto y ámbito, la ley establece las definiciones y principios generales que inspiran el concepto de Seguridad Nacional como Política de Estado, la Cultura de Seguridad Nacional, la cooperación con las Comunidades Autónomas, la colaboración privada, los componentes fundamentales, así como los ámbitos de especial interés y sus obligaciones.

En el título I se detallan cuáles son los órganos competentes de la Seguridad Nacional y qué competencias se les asignan en esta materia.

Por su parte, el título II se dedica a la creación y definición del Sistema de Seguridad Nacional, sus funciones y organización.

El título III regula la gestión de crisis, como marco general de funcionamiento del Sistema de Seguridad Nacional, y establece definiciones y competencias en dicha materia. La regulación de la situación de interés para la Seguridad Nacional prevé que no se ejerzan en ella las potestades propias de los estados de alarma y de excepción, de modo que si ello fuere necesario habría que proceder a su declaración y al sometimiento a su normativa específica.

Por último, el título IV regula la contribución de recursos a la Seguridad Nacional, que remite a una nueva ley a desarrollar.

La parte final de la ley incluye cuatro disposiciones adicionales sobre coordinación con instrumentos internacionales de gestión de crisis, homologación de instrumentos de gestión de crisis y comunicación pública respectivamente; una disposición transitoria relativa a la actividad de los Comités Especializados existentes a la entrada en vigor de esta ley; y cuatro disposiciones finales, que regulan los títulos competenciales, el desarrollo reglamentario, el mandato legislativo y la entrada en vigor.

TÍTULO PRELIMINAR

Disposiciones generales

Artículo 1. *Objeto.*

Esta ley tiene por objeto regular:

a) Los principios básicos, órganos superiores y autoridades y los componentes fundamentales de la Seguridad Nacional.
b) El Sistema de Seguridad Nacional, su dirección, organización y coordinación.
c) La gestión de crisis.
d) La contribución de recursos a la Seguridad Nacional.

Artículo 2. *Ámbito de aplicación.*

1. Esta ley será de aplicación a las diferentes Administraciones Públicas y, en los términos que en ella se establecen, a las personas físicas o jurídicas.
2. Los estados de alarma y excepción, se rigen por su normativa específica.

Artículo 3. *Seguridad Nacional.*

A los efectos de esta ley se entenderá por Seguridad Nacional la acción del Estado dirigida a proteger la libertad, los derechos y bienestar de los ciudadanos, a garantizar la defensa de España y sus principios y valores constitucionales, así como a contribuir junto a nuestros socios y aliados a la seguridad internacional en el cumplimiento de los compromisos asumidos.

Artículo 4. *Política de Seguridad Nacional.*

1. La Política de Seguridad Nacional es una política pública en la que bajo la dirección del Presidente del Gobierno y la responsabilidad del Gobierno, participan todas las Administraciones Públicas, de acuerdo con sus respectivas competencias, y la sociedad en general, para responder a las necesidades de la Seguridad Nacional.
2. Los principios básicos que orientarán la política de Seguridad Nacional son la unidad de acción, anticipación, prevención, eficiencia, sostenibilidad en el uso de los recursos, capacidad de resistencia y recuperación, coordinación y colaboración.
3. La Estrategia de Seguridad Nacional es el marco político estratégico de referencia de la Política de Seguridad Nacional. Contiene el análisis del entorno estratégico, concreta los riesgos y amenazas que afectan a la seguridad de España, define las líneas de acción estratégicas en cada ámbito de actuación y promueve la optimización de los recursos existentes. Se elabora a iniciativa del Presidente del Gobierno, quien la somete a la aprobación del Consejo de Ministros, y se revisará cada cinco años o cuando lo aconsejen las circunstancias cambiantes del entorno estratégico. Una vez aprobada, será presentada en las Cortes Generales en los términos previstos en esta ley.

Artículo 5. *Cultura de Seguridad Nacional.*

1. El Gobierno promoverá una cultura de Seguridad Nacional que favorezca la implicación activa de la sociedad en su preservación y garantía, como requisito indispensable para el disfrute de la libertad, la justicia, el bienestar, el progreso y los derechos de los ciudadanos.

2. A los efectos del número anterior, el Gobierno pondrá en marcha acciones y planes que tengan por objeto aumentar el conocimiento y la sensibilización de la sociedad acerca de los requerimientos de la Seguridad Nacional, de los riesgos y amenazas susceptibles de comprometerla, del esfuerzo de los actores y organismos implicados en su salvaguarda y la corresponsabilidad de todos en las medidas de anticipación, prevención, análisis, reacción, resistencia y recuperación respecto a dichos riesgos y amenazas.

Artículo 6. *Cooperación con las Comunidades Autónomas.*

1. La cooperación entre el Estado y las Comunidades Autónomas en las materias propias de esta ley, se realizará a través de la Conferencia Sectorial para asuntos de la Seguridad Nacional, todo ello sin perjuicio de las funciones asignadas al Consejo de Seguridad Nacional.

2. En particular, corresponderá a la Conferencia, como órgano de cooperación entre el Estado y las Comunidades Autónomas, el tratamiento y resolución con arreglo al principio de cooperación de aquellas cuestiones de interés común relacionadas con la Seguridad Nacional, como las siguientes:

a) Procedimientos técnicos para asegurar la recepción de la información sobre Seguridad Nacional de carácter general por parte de las Comunidades Autónomas, y la articulación de la información que éstas han de aportar al Estado.

b) Fórmulas de participación en los desarrollos normativos sobre Seguridad Nacional, mediante procedimientos internos que faciliten la aplicación de las actuaciones de la política de Seguridad Nacional, así como en la elaboración de los instrumentos de planificación que se prevea utilizar.

c) Problemas planteados en la ejecución de la política de Seguridad Nacional y el marco de las respectivas competencias estatutarias autonómicas.

3. La participación de las Ciudades con Estatuto de Autonomía de Ceuta y Melilla en los asuntos relacionados con la Seguridad Nacional también se articulará en la Conferencia, formando parte de la misma un representante de cada una de ellas.

4. Para su adecuado funcionamiento, la Conferencia elaborará un Reglamento interno. Los acuerdos de la Conferencia se adoptarán conforme a lo dispuesto en el artículo 5 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, y su Reglamento interno.

Artículo 7. *Colaboración privada.*

1. Las entidades privadas, siempre que las circunstancias lo aconsejen y, en todo caso, cuando sean operadoras de servicios esenciales y de infraestructuras críticas que puedan afectar a la Seguridad Nacional, deberán colaborar con las Administraciones Públicas. El Gobierno establecerá reglamentariamente los mecanismos y formas de esta colaboración.

2. El Gobierno, en coordinación con las Comunidades Autónomas, establecerá cauces que fomenten la participación del sector privado en la formulación y ejecución de la política de Seguridad Nacional.

Artículo 8. *Participación ciudadana en la Seguridad Nacional.*

El Gobierno, en coordinación con las Comunidades Autónomas, establecerá mecanismos que faciliten la participación de la sociedad civil y sus organizaciones en la formulación y la ejecución de la política de Seguridad Nacional.

Artículo 9. *Componentes fundamentales de la Seguridad Nacional.*

1. Se consideran componentes fundamentales de la Seguridad Nacional a los efectos de esta ley la Defensa Nacional, la Seguridad Pública y la Acción Exterior, que se regulan por su normativa específica.

2. Los Servicios de Inteligencia e Información del Estado, de acuerdo con el ámbito de sus competencias, apoyarán permanentemente al Sistema de Seguridad Nacional, proporcionando elementos de juicio, información, análisis, estudios y propuestas necesarios para prevenir y detectar los riesgos y amenazas y contribuir a su neutralización.

Artículo 10. *Ámbitos de especial interés de la Seguridad Nacional.*

Se considerarán ámbitos de especial interés de la Seguridad Nacional aquellos que requieren una atención específica por resultar básicos para preservar los derechos y libertades, así como el bienestar de los ciudadanos, y para garantizar el suministro de los servicios y recursos esenciales. A los efectos de esta ley, serán, entre otros, la ciberseguridad, la seguridad económica y financiera, la seguridad marítima, la seguridad del espacio aéreo y ultraterrestre, la seguridad energética, la seguridad sanitaria y la preservación del medio ambiente.

Artículo 11. *Obligaciones de las Administraciones Públicas en los ámbitos de especial interés.*

1. En el marco del Sistema de Seguridad Nacional, las Administraciones Públicas con competencias en los ámbitos de especial interés de la Seguridad Nacional, estarán obligadas a establecer mecanismos de coordinación e intercambio de información, especialmente en relación con los sistemas de vigilancia y alerta ante posibles riesgos y amenazas.
2. Asimismo, sin perjuicio de lo establecido en la normativa reguladora de protección de infraestructuras críticas, las Administraciones Públicas citadas anteriormente asegurarán la disponibilidad de los servicios esenciales y la garantía del suministro de recursos energéticos, agua y alimentación, medicamentos y productos sanitarios, o cualesquiera otros servicios y recursos de primera necesidad o de carácter estratégico.

TÍTULO I

Órganos competentes de la Seguridad Nacional

Artículo 12. *Órganos competentes en materia de Seguridad Nacional.*

1. Son órganos competentes en materia de Seguridad Nacional:

a) Las Cortes Generales.
b) El Gobierno.
c) El Presidente del Gobierno.
d) Los Ministros.
e) El Consejo de Seguridad Nacional.
f) Los Delegados del Gobierno en las Comunidades Autónomas y en las ciudades con Estatuto de Autonomía de Ceuta y Melilla.

2. A los efectos de esta ley, se entenderá que son órganos competentes de las Comunidades Autónomas y de las ciudades con Estatuto de Autonomía de Ceuta y Melilla, los que correspondan según lo dispuesto en cada Estatuto de Autonomía, en relación con las competencias que en cada caso estén relacionadas con la Seguridad Nacional.
3. Las autoridades locales ejercerán las competencias que les corresponden de acuerdo con esta ley y con lo dispuesto en la legislación de régimen local y demás leyes que les sean de aplicación.

Artículo 13. *Las Cortes Generales.*

1. Con independencia de las funciones que la Constitución y las demás disposiciones legales asignan a las Cortes Generales, les corresponde debatir las líneas generales de la política de Seguridad Nacional, a cuyos efectos el Gobierno presentará a las mismas, para su conocimiento y debate, la Estrategia de Seguridad Nacional, así como las iniciativas y planes correspondientes.
2. Se designará en las Cortes Generales una Comisión Mixta Congreso-Senado de Seguridad Nacional, siguiendo para ello lo dispuesto en los reglamentos de las Cámaras, con el fin de que las Cámaras tengan la participación adecuada en los ámbitos de la Seguridad Nacional y dispongan de la más amplia información sobre las iniciativas en el marco de la política de Seguridad Nacional. En el seno de esta Comisión Mixta comparecerá

anualmente el Gobierno, a través del representante que designe, para informar sobre la evolución de la Seguridad Nacional en dicho período de referencia. Asimismo, en esta Comisión Mixta será presentada la Estrategia de Seguridad Nacional y sus revisiones.

Artículo 14. *El Gobierno.*

Corresponde al Gobierno:

a) Establecer y dirigir la política de Seguridad Nacional y asegurar su ejecución.
b) Aprobar la Estrategia de Seguridad Nacional y sus revisiones mediante real decreto, en los términos previstos en esta ley.
c) Efectuar la Declaración de Recursos de Interés para la Seguridad Nacional en coordinación con las Comunidades Autónomas.

Artículo 15. *El Presidente del Gobierno.*

Corresponde al Presidente del Gobierno:

a) Dirigir la política de Seguridad Nacional y el Sistema de Seguridad Nacional.
b) Proponer la Estrategia de Seguridad Nacional y sus revisiones.
c) Declarar la Situación de Interés para la Seguridad Nacional.
d) Ejercer las demás competencias que en el marco del Sistema de Seguridad Nacional le atribuya esta ley, y las demás normas legales y reglamentarias que sean de aplicación.

Artículo 16. *Los Ministros.*

A los Ministros, como responsables de desarrollar la acción del Gobierno en las materias que les son propias, les corresponde desarrollar y ejecutar la política de Seguridad Nacional en los ámbitos de sus respectivos departamentos ministeriales.

Artículo 17. *El Consejo de Seguridad Nacional.*

El Consejo de Seguridad Nacional, en su condición de Comisión Delegada del Gobierno para la Seguridad Nacional, es el órgano al que corresponde asistir al Presidente del Gobierno en la dirección de la política de Seguridad Nacional y del Sistema de Seguridad Nacional, así como ejercer las funciones que se le atribuyan por esta ley y se le asignen por su reglamento.

TÍTULO II

Sistema de Seguridad Nacional

Artículo 18. *El Sistema de Seguridad Nacional.*

1. El Sistema de Seguridad Nacional es el conjunto de órganos, organismos, recursos y procedimientos, integrados en la estructura prevista en el artículo 20 de esta ley, que permite a los órganos competentes en materia de Seguridad Nacional ejercer sus funciones.
2. En el Sistema de Seguridad Nacional se integran los componentes fundamentales siguiendo los mecanismos de enlace y coordinación que determine el Consejo de Seguridad Nacional, actuando bajo sus propias estructuras y procedimientos. En función de las necesidades, podrán asignarse cometidos a otros organismos y entidades, de titularidad pública o privada.

Artículo 19. *Funciones.*

Al Sistema de Seguridad Nacional le corresponde evaluar los factores y situaciones que puedan afectar a la Seguridad Nacional, recabar y analizar la información que permita tomar las decisiones necesarias para dirigir y coordinar la respuesta ante las situaciones de crisis contempladas en esta ley, detectar las necesidades y proponer las medidas sobre planificación y coordinación con el conjunto de las Administraciones Públicas, con el fin de garantizar la disponibilidad y el correcto funcionamiento de los recursos del Sistema.

Artículo 20. *Estructura del Sistema de Seguridad Nacional.*

1. El Presidente del Gobierno dirige el Sistema asistido por el Consejo de Seguridad Nacional.
2. El Departamento de Seguridad Nacional ejercerá las funciones de Secretaría Técnica y órgano de trabajo permanente del Consejo de Seguridad Nacional y de sus órganos de apoyo, así como las demás funciones previstas en la normativa que le sea de aplicación.
3. Los órganos de apoyo del Consejo de Seguridad Nacional, con la denominación de Comités Especializados u otra que se determine, ejercen las funciones asignadas por el Consejo de Seguridad Nacional en los ámbitos de actuación previstos en la Estrategia de Seguridad Nacional, o cuando las circunstancias propias de la gestión de crisis lo precisen.
4. Será objeto de desarrollo reglamentario, en coordinación con las Administraciones Públicas afectadas, la regulación de los órganos de coordinación y apoyo del Departamento de Seguridad Nacional, así como de los mecanismos de enlace y coordinación permanentes con los organismos de todas las Administraciones del Estado que sean necesarios para que el Sistema de Seguridad Nacional pueda ejercer sus funciones y cumplir sus objetivos; todo ello sin perjuicio de las previsiones que en materia de gestión de crisis se contienen en el título III.

Artículo 21. *Funciones y composición del Consejo de Seguridad Nacional.*

1. Corresponde al Consejo de Seguridad Nacional ejercer las siguientes funciones:

a) Dictar las directrices necesarias en materia de planificación y coordinación de la política de Seguridad Nacional.
b) Dirigir y coordinar las actuaciones de gestión de situaciones de crisis en los términos previstos en el título III.
c) Supervisar y coordinar el Sistema de Seguridad Nacional.
d) Verificar el grado de cumplimiento de la Estrategia de Seguridad Nacional y promover e impulsar sus revisiones.
e) Promover e impulsar la elaboración de las estrategias de segundo nivel que sean necesarias y proceder, en su caso, a su aprobación, así como a sus revisiones periódicas.
f) Organizar la contribución de recursos a la Seguridad Nacional conforme a lo establecido en esta ley.
g) Aprobar el Informe Anual de Seguridad Nacional antes de su presentación en las Cortes Generales.
h) Acordar la creación y el fortalecimiento de los órganos de apoyo necesarios para el desempeño de sus funciones.
i) Impulsar las propuestas normativas necesarias para el fortalecimiento del Sistema de Seguridad Nacional.
j) Realizar las demás funciones que le atribuyan las disposiciones legales y reglamentarias que sean de aplicación.

2. A propuesta del Presidente del Gobierno, el Consejo de Seguridad Nacional informará al Rey al menos una vez al año. Cuando el Rey asista a las reuniones del Consejo, lo presidirá.
3. La composición del Consejo de Seguridad Nacional se determinará conforme a lo previsto en el apartado 8 de este artículo. En todo caso, deberán formar parte de dicho Consejo:

a) El Presidente del Gobierno, que lo presidirá.
b) Los Vicepresidentes del Gobierno, si los hubiere.
c) Los Ministros de Asuntos Exteriores y de Cooperación, de Justicia, de Defensa, de Hacienda y Administraciones Públicas, del Interior, de Fomento, de Industria, Energía y Turismo, de Presidencia, de Economía y Competitividad y de Sanidad, Servicios Sociales e Igualdad.
d) El Director del Gabinete de la Presidencia del Gobierno, el Secretario de Estado de Asuntos Exteriores, el Jefe de Estado Mayor de la Defensa, el Secretario de Estado de Seguridad y el Secretario de Estado-Director del Centro Nacional de Inteligencia.

4. El Director del Departamento de Seguridad Nacional será convocado a las reuniones del Consejo de Seguridad Nacional.

5. También podrán formar parte del Consejo, cuando sean convocados en función de los asuntos a tratar, los titulares de los demás departamentos ministeriales y las autoridades autonómicas afectadas en la toma de decisiones y actuaciones a desarrollar por parte del Consejo.

6. Sin perjuicio de lo establecido en los apartados 3 y 4, los titulares de los órganos superiores y directivos de la Administración General del Estado, de los organismos públicos, de las Comunidades Autónomas y de las ciudades con Estatuto de Autonomía, así como las autoridades de la Administración Local, serán convocados a las reuniones del Consejo cuando su contribución se considere necesaria, y en todo caso cuando los asuntos a tratar afecten a sus respectivas competencias.

7. Igualmente podrán ser convocadas aquellas personas físicas o jurídicas cuya contribución se considere relevante a la vista de los asuntos a tratar en el orden del día.

8. Mediante real decreto acordado en Consejo de Ministros, a propuesta del Presidente del Gobierno, se desarrollará la concreta composición, organización y funciones del Consejo de Seguridad Nacional, en el marco de lo dispuesto en esta ley.

TÍTULO III

Gestión de crisis en el marco del Sistema de Seguridad Nacional

Artículo 22. *Gestión de crisis.*

1. La gestión de crisis es el conjunto ordinario de actuaciones dirigidas a detectar y valorar los riesgos y amenazas concretos para la Seguridad Nacional, facilitar el proceso de toma de decisiones y asegurar una respuesta óptima y coordinada de los recursos del Estado que sean necesarios.

2. La gestión de crisis se desarrollará a través de instrumentos de prevención, detección, respuesta, retorno a la normalidad y evaluación. Su desarrollo será gradual e implicará a los diferentes órganos que componen la estructura del Sistema de Seguridad Nacional, según sus competencias y de acuerdo con la situación de crisis que se produzca. Asimismo, en la gestión de crisis participarán las autoridades de la Comunidad Autónoma que, en su caso, resulte afectada.

Artículo 23. *Situación de interés para la Seguridad Nacional.*

1. La gestión de crisis se desarrollará en la situación de interés para la Seguridad Nacional, adaptándose a las específicas circunstancias de la misma, de acuerdo con lo dispuesto en este título.

2. La situación de interés para la Seguridad Nacional es aquella en la que, por la gravedad de sus efectos y la dimensión, urgencia y transversalidad de las medidas para su resolución, requiere de la coordinación reforzada de las autoridades competentes en el desempeño de sus atribuciones ordinarias, bajo la dirección del Gobierno, en el marco del Sistema de Seguridad Nacional, garantizando el funcionamiento óptimo, integrado y flexible de todos los recursos disponibles, en los términos previstos en esta ley.

3. La situación de interés para la Seguridad Nacional se afrontará con los poderes y medios ordinarios de las distintas Administraciones Públicas y en ningún caso podrá implicar la suspensión de los derechos fundamentales y libertades públicas de los ciudadanos.

Artículo 24. *Declaración de la situación de interés para la Seguridad Nacional.*

1. La situación de interés para la Seguridad Nacional se declarará por el Presidente del Gobierno mediante real decreto. La declaración incluirá, al menos:

a) La definición de la crisis.
b) El ámbito geográfico del territorio afectado.
c) La duración y, en su caso, posible prórroga.

d) El nombramiento, en su caso, de una autoridad funcional, y la determinación de sus competencias para dirigir y coordinar las actuaciones que procedan.

e) La determinación de los recursos humanos y materiales necesarios para afrontar la situación de interés para la Seguridad Nacional, previstos en los correspondientes planes de preparación y disposición de recursos, así como de otros recursos adicionales que se requieran en cada caso, de acuerdo con lo dispuesto en el título IV.

2. La Declaración de situación de interés para la Seguridad Nacional supondrá la obligación de las autoridades competentes de aportar los medios humanos y materiales necesarios que se encuentren bajo su dependencia, para la efectiva aplicación de los mecanismos de actuación.

3. El Gobierno informará inmediatamente al Congreso de los Diputados de las medidas adoptadas y de la evolución de la situación de interés para la Seguridad Nacional.

Artículo 25. *Funciones del Consejo de Seguridad Nacional en la gestión de crisis.*

1. El Consejo de Seguridad Nacional determinará los mecanismos de enlace y coordinación necesarios para que el Sistema de Seguridad Nacional se active preventivamente y realice el seguimiento de los supuestos susceptibles de derivar en una situación de interés para la Seguridad Nacional.

2. En la situación de interés para la Seguridad Nacional el Presidente del Gobierno convocará al Consejo de Seguridad Nacional para que ejerza las funciones de dirección y coordinación de la gestión de dicha Situación, todo ello sin perjuicio de la aplicación de la legislación en materia de Defensa Nacional y de las competencias que correspondan al Consejo de Ministros. En los casos en los que el Presidente del Gobierno decida designar una autoridad funcional para el impulso y la gestión coordinada de las actuaciones, el Consejo de Seguridad Nacional asesorará sobre el nombramiento de dicha autoridad.

3. El Consejo de Seguridad Nacional asesorará al Presidente del Gobierno cuando la situación requiera la aplicación de medidas excepcionales previstas en los instrumentos de gestión de crisis de las organizaciones internacionales de las que España sea miembro, todo ello sin perjuicio de las facultades que corresponden al Consejo de Ministros y de lo previsto en la legislación en materia de Defensa Nacional.

Artículo 26. *Órganos de coordinación y apoyo del Consejo de Seguridad Nacional en materia de gestión de crisis.*

1. En materia de gestión de crisis el Consejo de Seguridad Nacional estará asistido por un Comité Especializado de carácter único para el conjunto del Sistema de Seguridad Nacional, para lo cual estará apoyado por el Departamento de Seguridad Nacional. Al citado Comité Especializado le corresponderá, entre otras funciones, elaborar propuestas de las directrices político-estratégicas y formular recomendaciones para la dirección de las situaciones de interés para la Seguridad Nacional. Será presidido por el miembro del Consejo de Seguridad Nacional o en su caso la autoridad funcional, que sea designado por el Presidente del Gobierno.

2. Los instrumentos preventivos de los órganos de coordinación y apoyo del Consejo de Seguridad Nacional podrán activarse anticipadamente, para llevar a cabo el análisis y seguimiento de los supuestos susceptibles de derivar en una situación de interés para la Seguridad Nacional. A estos efectos, todas las Administraciones y organismos públicos estarán obligados a colaborar de conformidad con lo previsto en esta ley.

TÍTULO IV

Contribución de recursos a la Seguridad Nacional

Artículo 27. *La contribución de recursos a la Seguridad Nacional en el Sistema de Seguridad Nacional.*

1. La aportación de recursos humanos y materiales, tanto públicos como privados, no adscritos con carácter permanente a la Seguridad Nacional, se basará en los principios de

contribución gradual y proporcionada a la situación que sea necesario afrontar y de indemnidad.

2. La organización de la contribución de recursos a la Seguridad Nacional recaerá en el Consejo de Seguridad Nacional, en coordinación con las Comunidades Autónomas, en los términos establecidos en esta ley y en las demás que sean de aplicación.

3. Las diferentes Administraciones Públicas, a través de sus órganos competentes, dispondrán de un sistema de identificación, evaluación y planificación de medios y recursos correspondientes a sus respectivos ámbitos competenciales, para hacer frente a los posibles riesgos o amenazas a la Seguridad Nacional.

4. Las Comunidades Autónomas y las Entidades Locales colaborarán en la elaboración de los planes de recursos humanos y materiales necesarios para las situaciones de crisis previstas en esta ley.

5. El sector privado participará en la contribución de recursos a la Seguridad Nacional.

6. El funcionamiento y organización de la contribución de recursos a la Seguridad Nacional se establecerá reglamentariamente de conformidad con lo previsto en esta ley.

Artículo 28. *Catálogo de recursos para la Seguridad Nacional.*

1. El Gobierno, mediante acuerdo del Consejo de Ministros, a propuesta del Consejo de Seguridad Nacional, procederá a aprobar un catálogo de recursos humanos y de medios materiales de los sectores estratégicos de la Nación que puedan ser puestos a disposición de las autoridades competentes en la situación de interés para la Seguridad Nacional. Su elaboración se realizará en coordinación con lo previsto en los catálogos sectoriales existentes en el conjunto de las Administraciones Públicas. A dichos efectos, las Comunidades Autónomas elaborarán los correspondientes catálogos de recursos en base a sus propias competencias y a la información facilitada por el Gobierno, los cuales se integrarán en el mencionado catálogo.

2. Dicho catálogo será actualizado cuando así se establezca por el Gobierno y, en todo caso, cada vez que se revise la Estrategia de Seguridad Nacional, de acuerdo con los nuevos riesgos y amenazas.

3. Una vez aprobado el catálogo, los componentes del Sistema de Seguridad Nacional establecerán las directrices y procedimientos para capacitar a personas y adecuar aquellos medios e instalaciones, públicos y privados, en caso de necesidad. A estos efectos, se elaborarán los planes de preparación y disposición de recursos para la Seguridad Nacional.

Artículo 29. *Declaración de recursos para la Seguridad Nacional.*

1. El Gobierno aprobará mediante real decreto la Declaración de Recursos que se podrán emplear en la situación de interés para la Seguridad Nacional prevista en esta ley. Dicho real decreto incluirá la relación de medios humanos y materiales, tanto públicos como privados, que procedan.

2. La disposición de recursos se efectuará mediante la adscripción al Sistema de Seguridad Nacional del personal, instalaciones y medios, según los planes activados para la situación de interés para la Seguridad Nacional prevista en esta ley. La adscripción de dichos recursos se realizará tal y como se establezca reglamentariamente, en coordinación con las Comunidades Autónomas.

3. Cualquier perjuicio que se ocasione como consecuencia de la declaración de recursos para la Seguridad Nacional dará lugar a la correspondiente indemnización, de acuerdo con lo dispuesto en las normas legales que resulten de aplicación y, en concreto, en los artículos 139 y siguientes de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Disposición adicional primera.

Los instrumentos de gestión de crisis y de la contribución de recursos del Sistema de Seguridad Nacional servirán de apoyo en los estados de alarma y de excepción de conformidad con su propia regulación específica, a decisión del Gobierno, y sin perjuicio de lo dispuesto en la legislación de Defensa nacional.

Disposición adicional segunda. *Coordinación con otros instrumentos internacionales de gestión de crisis.*

Las normas y procedimientos de gestión de crisis del Sistema de Seguridad Nacional deberán ser compatibles y homologables con los instrumentos de gestión de crisis de las organizaciones internacionales en las que España es parte.

Disposición adicional tercera. *Homologación de los instrumentos de gestión de crisis.*

Los órganos competentes de las distintas Administraciones públicas revisarán, en el plazo de seis meses desde la entrada en vigor de esta ley, sus normas y procedimientos de actuación para adecuar y coordinar su funcionamiento en el Sistema de Seguridad Nacional.

Disposición adicional cuarta. *Comunicación pública.*

El Sistema de Seguridad Nacional deberá contar con una política informativa para situaciones de crisis, cuya coordinación estará a cargo de la autoridad que ejerza de Portavoz del Gobierno.

Disposición transitoria única. *Actividad de los Comités Especializados existentes a la entrada en vigor de esta ley y procedimientos de actuación.*

1. Los Comités Especializados del Consejo de Seguridad Nacional existentes a la entrada en vigor de esta ley, continuarán desarrollando sus funciones de acuerdo con los respectivos acuerdos de constitución hasta que sean adaptados a lo dispuesto en esta ley, lo cual deberá hacerse en el plazo de tres meses desde su entrada en vigor.
2. En particular, en este proceso de adaptación de los acuerdos de constitución de los Comités Especializados mencionados en el apartado anterior, se impulsará la adaptación o preparación de los procedimientos necesarios para coordinar sus actuaciones con cuantos otros órganos colegiados o grupos dependientes de estos confluyan en la gestión de crisis, en el marco de lo previsto en los artículos 18.2 y 22.

Disposición final primera. *Títulos competenciales.*

Esta ley se dicta al amparo de lo dispuesto en el artículo 149.1.4.ª y 29.ª de la Constitución que atribuyen al Estado la competencia exclusiva en materia de defensa y Fuerzas Armadas y en materia de seguridad pública.

Disposición final segunda. *Desarrollo reglamentario.*

Se faculta al Gobierno y a los titulares de los departamentos ministeriales, en el ámbito de sus respectivas competencias, para dictar cuantas disposiciones sean necesarias para la ejecución y desarrollo de lo establecido en esta ley.

Disposición final tercera. *Mandato legislativo.*

El Gobierno, en el plazo de un año desde la entrada en vigor de esta ley, deberá remitir al Congreso de los Diputados un proyecto de ley reguladora de la preparación y disposición de la contribución de recursos a la Seguridad Nacional.

Disposición final cuarta. *Entrada en vigor.*

La presente ley entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

§ 4

Orden PRA/33/2018, de 22 de enero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se regula el Consejo Nacional de Ciberseguridad

Ministerio de la Presidencia y para las Administraciones Territoriales
«BOE» núm. 20, de 23 de enero de 2018
Última modificación: sin modificaciones
Referencia: BOE-A-2018-799

El Consejo de Seguridad Nacional, en su reunión de 1 de diciembre de 2017, ha adoptado un Acuerdo por el que se regula el Consejo Nacional de Ciberseguridad.

Para general conocimiento, y en cumplimiento de lo dispuesto en el apartado segundo del propio Acuerdo, se dispone su publicación como Anejo a la presente Orden.

ANEJO

Acuerdo por el que se regula el Consejo Nacional de Ciberseguridad

Exposición

La disposición transitoria única de la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, dispone que los Comités Especializados del Consejo de Seguridad Nacional existentes a su entrada en vigor, continuarán desarrollando sus funciones de acuerdo con los respectivos acuerdos de constitución hasta que sean adaptados a lo dispuesto en la misma.

Por otra parte, la Ley de Seguridad Nacional, además de asignar funciones concretas a los órganos competentes de la Seguridad Nacional, entre los cuales se encuentran las Cortes Generales, el Gobierno, el Presidente del Gobierno, los Ministros, el Consejo de Seguridad Nacional, los Delegados del Gobierno en las Comunidades Autónomas y en las ciudades con Estatuto de Autonomía de Ceuta y Melilla, así como los órganos que correspondan de las distintas Comunidades Autónomas según lo dispuesto en los respectivos Estatutos de Autonomía en conexión con las competencias relacionadas con la Seguridad Nacional y las autoridades locales, configura el concepto, las funciones y la estructura del Sistema de Seguridad Nacional con plena observancia del orden constitucional, tal como ha señalado el Tribunal Constitucional en la sentencia de 3 de noviembre de 2016.

Precisamente es en la estructura del Sistema de Seguridad Nacional donde los órganos de apoyo del Consejo de Seguridad Nacional hallan la razón de su existencia, como órganos dependientes del Consejo de Seguridad Nacional en su condición de Comisión Delegada del Gobierno para la Seguridad Nacional al que corresponde asistir al Presidente del Gobierno en la dirección de la política de Seguridad Nacional y del Sistema de Seguridad Nacional y en las demás funciones que el ordenamiento jurídico le atribuya.

El carácter instrumental de los órganos de apoyo del Consejo de Seguridad Nacional ya existentes de acuerdo con la regulación contenida en el Real Decreto 385/2013, de 31 de mayo, de modificación del Real Decreto 1886/2011, de 30 de diciembre, por el que se establecen las Comisiones Delegadas del Gobierno, se consolida en la Ley de Seguridad Nacional que, en concreto, en su artículo 20.3, prevé que estos órganos de apoyo con la denominación de Comités Especializados u otra que se determine, ejercen las funciones asignadas por el Consejo de Seguridad Nacional en los ámbitos de actuación previstos en la Estrategia de Seguridad Nacional, o cuando las circunstancias propias de la gestión de crisis lo precisen.

Para facilitar el ejercicio de las funciones del Consejo de Seguridad Nacional en el campo concreto de la ciberseguridad, al que la Ley de Seguridad Nacional considera un ámbito de especial interés para la Seguridad Nacional, cuyos objetivos y líneas de acción se han concretado en la Estrategia de Ciberseguridad Nacional, y así cumplir con el mandato de la Disposición transitoria única, siguiendo asimismo las directrices para la regulación de los órganos de apoyo del Consejo de Seguridad Nacional dictadas por el citado Consejo en el Acuerdo de 20 de enero de 2017, es necesario actualizar el Acuerdo de 5 de diciembre de 2013, por el que se adopta la iniciativa para la creación del Comité Especializado de Ciberseguridad, constituido bajo la denominación de Consejo Nacional de Ciberseguridad.

En particular, la puesta al día abarcará lo relacionado con su naturaleza jurídica, el régimen jurídico aplicable, las funciones específicas, la composición y, concretamente, el régimen de su presidencia y procedimiento de designación de sus miembros, además de otras previsiones, como la emisión de informes y finalidad de los mismos, la creación de grupos de trabajo y, por último, el reforzamiento del enlace y coordinación con los componentes fundamentales y ámbitos de especial interés para la Seguridad Nacional dentro del marco del Sistema de Seguridad Nacional de conformidad con lo dispuesto en el Acuerdo del Consejo de 20 de enero de 2017, de implementación de los mecanismos para garantizar el funcionamiento integrado del Sistema de Seguridad Nacional.

En su virtud, en aplicación de lo dispuesto en la Disposición transitoria única de la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, en conexión con el artículo 21.1.h) de dicha Ley, y de conformidad con el Acuerdo del Consejo de Seguridad Nacional de 20 de enero de 2017, por el que se dictan directrices para la regulación de los órganos de apoyo, el Consejo de Seguridad Nacional, en su reunión del día 1 de diciembre de 2017, ha adoptado el siguiente Acuerdo:

ACUERDO

Primero.

Se modifica el marco regulador del Consejo Nacional de Ciberseguridad aprobado por Acuerdo del Consejo de Seguridad Nacional en su reunión del día 5 de diciembre de 2013, que queda redactado en la forma en que se recoge en el anexo al presente Acuerdo.

Segundo.

Este Acuerdo se publicará en el «Boletín Oficial del Estado», en la página web del Departamento de Seguridad Nacional www.dsn.gob.es y en las sedes electrónicas de los órganos y organismos a los que sea de aplicación y producirá efectos desde el día siguiente al de su publicación en el «Boletín Oficial del Estado».

ANEXO

Acuerdo por el que se regula el Consejo Nacional de Ciberseguridad

Primero. *Objeto.*

El presente Acuerdo tiene por objeto establecer el marco regulador del Consejo Nacional de Ciberseguridad (en adelante el Consejo) de conformidad con lo dispuesto en la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional y en las demás normas que resulten

de aplicación, en su condición de órgano de apoyo del Consejo de Seguridad Nacional en el marco del Sistema de Seguridad Nacional.

Segundo. *Naturaleza jurídica.*

El Consejo es un órgano de apoyo del Consejo de Seguridad Nacional de los previstos en el artículo 20.3 de la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, al que corresponde ejercer las funciones asignadas por aquel en el ámbito de la ciberseguridad y en el marco del Sistema de Seguridad Nacional, según se concretan en este Acuerdo.

Tercero. *Régimen jurídico aplicable.*

El Consejo se rige por lo dispuesto en la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, por el presente Acuerdo y por sus Normas de régimen interno y de funcionamiento. En su defecto, por lo dispuesto en las instrucciones que han de seguirse para la tramitación de asuntos ante los órganos colegiados del Gobierno y en la legislación básica sobre régimen jurídico del sector público, que resulte de aplicación.

Cuarto. *Funciones específicas.*

El Consejo ejercerá las siguientes funciones:

1. Proponer al Consejo de Seguridad Nacional las directrices en materia de planificación y coordinación de la política de Seguridad Nacional relacionadas con la ciberseguridad.
2. Contribuir a reforzar el adecuado funcionamiento del Sistema de Seguridad Nacional en el ámbito de la ciberseguridad, cuya supervisión y coordinación corresponde al Consejo de Seguridad Nacional.
3. Apoyar al Consejo de Seguridad Nacional en su función de verificar el grado de cumplimiento de la Estrategia de Seguridad Nacional y proponer, en su caso, su revisión, en lo relacionado con la ciberseguridad.
4. Verificar el grado de cumplimiento de la Estrategia de Ciberseguridad Nacional, así como de los instrumentos de desarrollo aprobados, para ulterior informe al Consejo de Seguridad Nacional, con propuestas para una posible revisión de la existente o aprobación de una nueva estrategia sectorial.
5. Contribuir a la elaboración de propuestas normativas para el fortalecimiento del Sistema de Seguridad Nacional en el ámbito de la ciberseguridad.
6. Apoyar la toma de decisiones del Consejo de Seguridad Nacional en las materias propias del ámbito de la ciberseguridad, mediante el análisis, estudio y propuesta de iniciativas tanto en el ámbito nacional como en el internacional.
7. Reforzar las relaciones con las Administraciones Públicas concernidas en el ámbito de la ciberseguridad, así como la coordinación, colaboración y cooperación entre los sectores público y privado.
8. Realizar en apoyo del Comité Especializado de Situación la valoración de los riesgos y amenazas, analizar los posibles escenarios de crisis, en especial de aquellos susceptibles de derivar en una situación de interés para la Seguridad Nacional, en el ámbito de la ciberseguridad, y evaluar los resultados de su ejecución, todo ello en coordinación con los órganos y autoridades directamente competentes y con el Comité Especializado de Situación.
9. Contribuir a la organización de la contribución de recursos a la Seguridad Nacional de responsabilidad del Consejo de Seguridad Nacional en el ámbito de la ciberseguridad.
10. Aprobar sus propias normas de régimen interno y de funcionamiento.
11. Todas aquellas otras funciones que le atribuya el ordenamiento jurídico o que le encomiende el Consejo de Seguridad Nacional.

Quinto. *Composición.*

a) Presidencia:

La presidencia será ejercida por el Secretario de Estado Director del Centro Nacional de Inteligencia.

Corresponde al Presidente:

– Ostentar la representación del órgano y, en particular, canalizar los informes del Consejo Nacional de Ciberseguridad para el Consejo de Seguridad Nacional.

– Acordar la convocatoria de las sesiones ordinarias y extraordinarias y la fijación del orden del día en los términos señalados en las Normas de régimen interno y de funcionamiento.

– Presidir las reuniones, moderar el desarrollo de los debates y acordar su suspensión por causas justificadas.

– Asegurar el cumplimiento de las leyes.

– Visar las actas y certificaciones de los acuerdos del órgano.

– Velar por la búsqueda del consenso para la adopción de acuerdos.

– En caso de llevarse a cabo votación para la adopción de un acuerdo, de conformidad con las Normas de régimen interno y de funcionamiento, dirimirá con su voto los empates.

– Las demás funciones previstas en las normas legales y reglamentarias que resulten aplicables y, en particular, en las Normas de régimen interno y de funcionamiento del Consejo.

b) Vicepresidencia:

La Vicepresidencia será ocupada por el Director del Departamento de Seguridad Nacional.

Corresponderá al Vicepresidente sustituir al Presidente en los casos de vacante, ausencia, enfermedad u otra causa legal, y en su defecto, por el miembro de mayor jerarquía, antigüedad y edad, por este orden.

c) Vocales:

1. El Comité estará compuesto por un vocal con rango mínimo de Subdirector general o asimilado u Oficial General de cada departamento ministerial y organismo público con representación en el Consejo de Seguridad Nacional, que será designado por el titular del ministerio y organismo respectivo.

2. Asimismo, podrá formar parte del Consejo un representante del resto de los departamentos ministeriales u organismos públicos cuya presencia sea así acordada por el Presidente, en función de los asuntos a tratar.

3. Serán convocados, además, los titulares de los órganos superiores y directivos de la Administración General del Estado, las autoridades competentes de las Comunidades Autónomas, de las ciudades con Estatuto de Autonomía, de la Administración Local, así como de los organismos públicos y entidades de derecho público vinculados o dependientes de las Administraciones Públicas, cuando su contribución se considere necesaria y, en todo caso, cuando los asuntos a tratar afecten a sus respectivas competencias. Igualmente, podrán ser convocados representantes de las demás entidades que integran el sector público institucional, del sector privado y aquellas personas en su condición de expertos cuya contribución se considere relevante.

4. El Consejo podrá ser convocado por el Presidente en composición reducida de acuerdo con las circunstancias concurrentes y el orden del día fijado para la reunión.

5. Los miembros del Consejo no podrán atribuirse las funciones de representación asignadas en su condición de órgano de apoyo, salvo que expresamente se les hayan reconocido por una norma o por acuerdo expresamente así adoptado para cada caso en particular, por el propio Consejo.

d) Secretaría Técnica y órgano de trabajo permanente del Consejo y otros apoyos a la presidencia:

1. Las funciones de Secretaría Técnica y órgano de trabajo permanente del Consejo serán desempeñadas por el Departamento de Seguridad Nacional. En este campo, le corresponderá efectuar la coordinación necesaria para que el Consejo en el ámbito de sus funciones preste el apoyo necesario al Consejo de Seguridad Nacional, asumiendo, en este contexto, el punto de enlace único entre el citado Consejo y el presente órgano de apoyo.

2. El Secretario será designado por el Presidente, a propuesta del Director del Departamento de Seguridad Nacional, entre el personal perteneciente a dicho Departamento.

3. En apoyo a la presidencia, el Presidente podrá recabar los apoyos necesarios de su propia estructura, en especial en todo lo relacionado con la organización de las reuniones del Consejo, bajo la coordinación del Departamento de Seguridad Nacional.

Sexto. *Emisión de informes.*

1. Los informes únicamente podrán ser emitidos a instancia del Consejo de Seguridad Nacional o a iniciativa del propio Consejo.
2. En todo caso, serán elevados a la consideración y, en su caso, conformidad del Consejo de Seguridad Nacional, a través del Presidente.

Séptimo. *Utilización de los mecanismos de enlace y coordinación.*

1. El Consejo utilizará los mecanismos de enlace y coordinación que en cumplimiento a lo dispuesto en la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, ha establecido el Consejo de Seguridad Nacional en el Acuerdo de 20 de enero de 2017, de implementación de los mecanismos para garantizar el funcionamiento integrado del Sistema de Seguridad Nacional, así como aquellos otros que se determinen en cumplimiento de lo dispuesto en la mencionada Ley.
2. De acuerdo con lo dispuesto en el apartado quinto del citado Acuerdo del Consejo de Seguridad Nacional de 20 de enero de 2017, los miembros del Consejo velarán por la coherencia y armonización de la información a trasladar en el seno del Consejo, para lo cual se coordinarán con sus respectivos puntos de contacto de Seguridad Nacional, dando así cumplimiento a los principios y procedimientos de actuación previstos en el mencionado Acuerdo.
3. El Departamento de Seguridad Nacional, de acuerdo con lo establecido en el artículo 20.4 de la Ley 36/2015, de 28 de septiembre, mantendrá activados los mecanismos de enlace y coordinación permanentes con los organismos del conjunto de las Administraciones Públicas que sean necesarios para que el Sistema de Seguridad Nacional ejerza sus funciones y cumpla con sus objetivos, de manera continua y sin perjuicio de las funciones que correspondan al Comité Especializado de Situación en materia de gestión de crisis.

Octavo. *Grupos de trabajo.*

1. El Consejo podrá crear grupos de trabajo para la asistencia técnica en el desempeño de sus funciones, con la composición, objetivos, cometidos y calendario para su realización, que para cada caso se disponga. Los grupos de trabajo podrán incorporar a expertos en la materia o recabar su criterio e invitar a participar en sus actividades a representantes de las Administraciones Públicas y del sector público y privado.
2. Los grupos de trabajo responderán ante el Consejo del resultado de sus cometidos y actividades que desarrollen, y serán coordinados por el Departamento de Seguridad Nacional.
3. El régimen de funcionamiento de los grupos de trabajo que se constituyan se determinará en las normas de régimen interno de las que se doten. En lo no previsto, se tendrá en cuenta lo dispuesto en la Sección 3.ª del Capítulo II del Título Preliminar de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Noveno. *Reuniones.*

El Consejo se reunirá con carácter presencial o a distancia a iniciativa de su Presidente como mínimo con carácter bimestral, o cuantas veces lo considere oportuno, atendiendo a las circunstancias que en materia de ciberseguridad demande la Seguridad Nacional, todo ello de acuerdo con lo dispuesto en este Acuerdo y en las Normas de régimen interno y de funcionamiento del Consejo.

§ 5

Orden PRA/116/2017, de 9 de febrero, por la que se publica el Acuerdo del Consejo Seguridad Nacional de implementación de los mecanismos para garantizar el funcionamiento integrado del Sistema de Seguridad Nacional

Ministerio de la Presidencia y para las Administraciones Territoriales
«BOE» núm. 38, de 14 de febrero de 2017
Última modificación: sin modificaciones
Referencia: BOE-A-2017-1460

El Consejo de Seguridad Nacional, en su reunión de 20 de enero de 2017, ha adoptado un Acuerdo de implementación de los mecanismos para garantizar el funcionamiento integrado del Sistema de Seguridad Nacional.

Para general conocimiento y en cumplimiento de lo dispuesto en el apartado segundo del propio Acuerdo, se dispone su publicación como Anejo a la presente Orden.

ANEJO

Acuerdo de implementación de los mecanismos para garantizar el funcionamiento integrado del Sistema de Seguridad Nacional

La Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, además de definir la Seguridad Nacional como la acción del Estado dirigida a proteger la libertad, los derechos y bienestar de los ciudadanos, a garantizar la defensa de España y sus principios y valores constitucionales, así como a contribuir junto a nuestros socios y aliados a la seguridad internacional en el cumplimiento de los compromisos asumidos, de establecer los principios básicos de la política de Seguridad Nacional y su marco estratégico de referencia, de encauzar y garantizar la participación del conjunto de las Administraciones Públicas en los asuntos propios de dicha política pública de nuevo cuño y, en definitiva, de estructurar la organización y funcionamiento del Sistema de Seguridad Nacional como principal apoyo del Gobierno a la hora de impulsar el enfoque integral de la gestión de crisis, prevé de manera taxativa la conexión de los denominados componentes fundamentales de la Seguridad Nacional, en concreto, la Defensa Nacional, la Seguridad Pública y la Acción Exterior, con el apoyo permanente de los servicios de inteligencia e información del Estado, tanto para su funcionamiento con carácter habitual, tal como se infiere del artículo 18.2 del citado texto legal, como para su utilización en los supuestos de gestión de crisis en el marco del Sistema de Seguridad Nacional.

Es decir, nos hallamos ante un mandato legal que atañe principalmente al Consejo de Seguridad Nacional como órgano colegiado del Gobierno, al que corresponde supervisar y coordinar el Sistema de Seguridad Nacional, con la finalidad de garantizar su adecuado funcionamiento como eje vertebrador de la ejecución de la política de Seguridad Nacional

por cada uno de los órganos competentes en la materia, y en cuya cúspide se sitúa el Presidente del Gobierno a quien corresponde la dirección del Sistema asistido por el Consejo de Seguridad Nacional.

La Ley de Seguridad Nacional también contempla en el artículo 11.1, el mandato para que las respectivas Administraciones Públicas competentes en cada uno de los ámbitos de especial interés para la Seguridad Nacional –recogidos con carácter enunciativo en el artículo 10- establezcan los mecanismos de coordinación e intercambio de información con el Sistema de Seguridad Nacional y, muy especialmente, en relación con los sistemas de vigilancia y alerta ante posibles riesgos y amenazas. El cumplimiento de dicho mandato legal se considera en estos momentos condicionado por dos factores que en un horizonte temporal posterior se podrían abordar conjuntamente: el primero la constitución de la Conferencia Sectorial para asuntos de la Seguridad Nacional como instrumento esencial de cooperación con las Comunidades Autónomas, y el segundo, la realización de los trabajos necesarios para abordar la homologación de los instrumentos de gestión de crisis de la Disposición adicional tercera de la referida Ley, ambos factores estrechamente ligados entre sí para encauzar la participación de la Administración Autonómica en la implementación de los mecanismos que sustenten el Sistema de Seguridad Nacional, lo que además, sintoniza a la perfección con la doctrina del Tribunal Constitucional expresada en la sentencia de 3 de noviembre de 2016 y que reafirma la constitucionalidad de los artículos 4.3, 15.b) y 24.2 de la Ley de Seguridad Nacional, todo lo cual da como resultante la necesidad de afrontar en una segunda fase la concreción de los mecanismos de enlace y coordinación del conjunto de las Administraciones Públicas, una vez homologados, con el Sistema de Seguridad Nacional, abordándose en este momento la integración en dicho Sistema de los correspondientes a los ámbitos competenciales de la Administración General del Estado en la triple dimensión antes apuntada:

a) Los mecanismos de enlace y coordinación de los componentes fundamentales de la Seguridad Nacional (artículo 18.2).

b) Los mecanismos de coordinación e intercambio de información de los ámbitos de especial interés que recaigan de competencia de la Administración General del Estado (artículo 11.1).

c) Los mecanismos de enlace y coordinación necesarios para que el Sistema de Seguridad Nacional se active preventivamente en los supuestos de gestión de crisis (artículo 25.1 en conexión con el artículo 19).

Hecha esta delimitación temporal y material del objeto del presente Acuerdo, es de destacar que a la vista de las funciones que el artículo 19 de la Ley de Seguridad Nacional atribuye al Sistema de Seguridad Nacional, así como de su propia estructura interna de conformidad con lo dispuesto en el artículo 20 del mismo texto legal, se considera que los mecanismos deben entenderse como una combinación entre la conformación de un conjunto de puntos focales ministeriales con asignación de funciones de apoyo en materia de Seguridad Nacional, y de procedimientos ágiles y eficaces que garanticen el funcionamiento óptimo, integrado y flexible del Sistema de Seguridad Nacional en el cumplimiento de sus funciones en cualquier escenario.

Estos mecanismos deben ser versátiles, adaptables a las necesidades demandadas por el Sistema que permitan tanto su utilización con carácter habitual para afrontar tareas de diversa naturaleza en materia de Seguridad Nacional, como en los supuestos de gestión de crisis en todas sus fases de acuerdo con las previsiones del Título III de la referida Ley, en conexión con lo dispuesto en su Disposición Transitoria única, apartado 2, y aprovechables tanto en apoyo al Consejo de Seguridad Nacional, como también a sus órganos de apoyo.

Por su parte, el Departamento de Seguridad Nacional en su condición de órgano de asesoramiento al Presidente del Gobierno en materia de Seguridad Nacional y Secretaría Técnica y órgano de trabajo permanente del Consejo de Seguridad Nacional, de acuerdo con su norma orgánica reguladora, es el centro neurálgico en el que deben entroncar los mecanismos de enlace y coordinación permanente con las Administraciones Públicas de acuerdo con lo dispuesto en el artículo 20.4 de la Ley de Seguridad Nacional, esto es, donde residan las terminales del conjunto de los puntos de contacto ministeriales y de los organismos públicos concernidos y el soporte de los procedimientos que materialicen las

conexiones entre el Sistema y los órganos competentes de la Seguridad Nacional, de modo que permanentemente fluya la información necesaria para la toma de decisiones en cualquier situación, afianzándose la fluidez en la transmisión de la información necesaria al Departamento de Seguridad Nacional por parte de las Administraciones Públicas concernidas a través de los mecanismos que entroncan en su estructura, extendiendo su radio de acción a los ámbitos de la sociedad civil que se consideren necesarios.

En su virtud, en aplicación de lo dispuesto en los artículos 18.2, 25.1, 21.1c), 22 y Disposición Transitoria única, apartado 2, en conexión con el artículo 11.1, todos ellos de la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, el Consejo de Seguridad Nacional, en su reunión del día 20 de enero de 2017, ha adoptado el siguiente Acuerdo:

Primero.

Se aprueba la implementación de los mecanismos para garantizar el funcionamiento integrado del Sistema de Seguridad Nacional, en los términos que figuran como Anexo.

Segundo.

El presente Acuerdo se publicará en el «Boletín Oficial del Estado», en la página web del Departamento de Seguridad Nacional www.dsn.gob.es y en las sedes electrónicas de los órganos y organismos a los que sea de aplicación y producirá efectos desde el día siguiente al de su publicación en el «Boletín Oficial del Estado».

ANEXO

Acuerdo de implementación de los mecanismos para garantizar el funcionamiento integrado del Sistema de Seguridad Nacional

Primero. *Objeto.*

El presente Acuerdo tiene por objeto designar los mecanismos del Sistema de Seguridad Nacional, que garanticen su óptimo funcionamiento con carácter habitual, y específicamente, en gestión de crisis, de acuerdo con las previsiones del Título III de la Ley de Seguridad Nacional.

Segundo. *Ámbito de aplicación.*

El presente Acuerdo se aplicará a los órganos de los departamentos ministeriales del Gobierno y organismos públicos y entidades de derecho público vinculados o dependientes de la Administración General del Estado, con o sin representación en el Consejo de Seguridad Nacional y, a través suyo, al conjunto de la Administración General del Estado.

Tercero. *Mecanismos del Sistema de Seguridad Nacional.*

1. El funcionamiento óptimo, integrado y flexible del Sistema de Seguridad Nacional en el cumplimiento de sus funciones ante cualquier escenario se sustenta en la concreción de diversos mecanismos, entendidos como una combinación de puntos focales ministeriales con asignación de funciones de apoyo en materia de Seguridad Nacional, y de procedimientos ágiles y eficaces que garanticen el intercambio fluido de información entre los órganos de la estructura del Sistema, cuyo punto central de enlace se constituye en el Departamento de Seguridad Nacional, y los órganos competentes de la Seguridad Nacional.

2. Los mecanismos del Sistema de Seguridad Nacional que se designan en el presente Acuerdo, se interrelacionarán en todos los ámbitos de la Seguridad Nacional y, en especial, en los relacionados con los componentes fundamentales de la Seguridad Nacional establecidos en el artículo 9 de la Ley de Seguridad Nacional, con los ámbitos de especial interés enunciados en su artículo 10 de competencia de los departamentos ministeriales y de los organismos públicos y entidades de derecho público vinculados o dependientes de la Administración General del Estado y, por último, con los más específicamente utilizables en materia de gestión de crisis, incluidos otros órganos colegiados o grupos dependientes de estos que confluyan en la gestión de crisis.

3. Los mecanismos que se designan deben ser capaces de adaptarse con facilidad y rapidez a las diversas funciones que se les encomienden conforme al presente Acuerdo, a lo dispuesto en la Ley de Seguridad Nacional, y en su propia regulación orgánica.

Cuarto. *Clases de mecanismos del Sistema de Seguridad Nacional.*

La tipología de los mecanismos del Sistema de Seguridad Nacional es la siguiente:

a) Mecanismos de enlace y coordinación permanente:

Se constituye una red de puntos de contacto de Seguridad Nacional compuesta por los Directores de Gabinete de los ministerios y organismos públicos pertenecientes al Consejo de Seguridad Nacional, bajo la coordinación del Departamento de Seguridad Nacional. Asimismo, estarán apoyados permanentemente por los respectivos centros de crisis de carácter ministerial y de otros organismos públicos dependientes.

b) Mecanismos de enlace y coordinación reforzada:

La red de puntos de contacto prevista en el apartado anterior será reforzada con la incorporación de representantes de los demás ministerios y organismos públicos y entidades de derecho público vinculados o dependientes de la Administración General del Estado no representados habitualmente en el Consejo de Seguridad Nacional, cuando así lo exijan las circunstancias que afecten a la Seguridad Nacional, incluidos los sectores de la sociedad civil cuya colaboración se requiera, de acuerdo con lo dispuesto en el artículo 7 de la Ley de Seguridad Nacional.

c) Coordinación del conjunto de los mecanismos de enlace y coordinación:

El Departamento de Seguridad Nacional efectuará la coordinación del conjunto de los mecanismos de enlace y coordinación del Sistema de Seguridad Nacional de conformidad con lo dispuesto en el artículo 20.4 de la Ley de Seguridad Nacional, y con lo establecido en su regulación orgánica específica y en el presente Acuerdo.

Quinto. *Principios y procedimientos de actuación.*

1. Los principios que regirán la actuación de los puntos de contacto de Seguridad Nacional serán, además, de los generales de la organización del sector público y básicos de la política de Seguridad Nacional, previstos respectivamente, en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y en la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, los siguientes:

a) Inmediatez en la respuesta.
b) Visión sectorial y armonizada examinada desde la perspectiva integral de la Seguridad Nacional.
c) Actualización permanente de la información y de la operatividad de los puntos de contacto.
d) Simplicidad en los procedimientos.
e) Carácter preferente de la comunicación directa y a través de videoconferencia y otros medios electrónicos.

2. El procedimiento habitual estará basado en el traslado de la información ordinaria de carácter sectorial por los puntos de contacto de Seguridad Nacional al Departamento de Seguridad Nacional, sin perjuicio de las atribuciones de los titulares de los ministerios y de los organismos públicos con representación en el Consejo de Seguridad Nacional y, en su caso, en su composición ampliada, así como de la respectiva representación en los órganos de apoyo del Consejo de Seguridad Nacional. Para ello, se viabilizará la celebración periódica y, al menos, una vez al mes, de una conferencia de Seguridad Nacional con participación de los puntos de contacto de Seguridad Nacional, o de la autoridad que se designe, mediante videoconferencia que garantice la interoperabilidad de todos los sistemas utilizados conectados con el Departamento de Seguridad Nacional, en especial con los sistemas de las salas y centros de crisis existentes en los ministerios y demás organismos públicos implicados.

3. El procedimiento específico a utilizar cuando las circunstancias que afecten a la Seguridad Nacional lo exijan, o cuando así lo acuerde el Presidente del Gobierno, se basará en los postulados del procedimiento habitual antes reseñado, al cual se añade la interconexión necesaria con el Comité Especializado de Situación, órgano de apoyo del Consejo de Seguridad Nacional de carácter único para el conjunto del Sistema de Seguridad Nacional y que asiste al Consejo en sus funciones asignadas en materia de gestión de crisis, a través del Centro de Situación del Departamento de Seguridad Nacional.

Sexto. *Informes periódicos al Consejo de Seguridad Nacional.*

El Director del Departamento de Seguridad Nacional informará al Consejo de Seguridad Nacional con carácter anual o, en cualquier momento si las circunstancias concurrentes así lo exigieran, en relación a la aplicación de lo dispuesto en el presente Acuerdo.

§ 6

Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad

Ministerio de Asuntos Económicos y Transformación Digital
«BOE» núm. 106, de 4 de mayo de 2022
Última modificación: 6 de noviembre de 2024
Referencia: BOE-A-2022-7191

I

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (en adelante, ENS) tenía por objeto determinar la política de seguridad en la utilización de medios electrónicos de las entidades de su ámbito de aplicación, estando constituido por los principios básicos y requisitos mínimos que han venido garantizando adecuadamente la seguridad de la información tratada y los servicios prestados por dichas entidades.

El ENS, cuyo ámbito de aplicación comprendía todas las entidades de las administraciones públicas, perseguía fundamentar la confianza en que los sistemas de información prestan sus servicios adecuadamente y custodian la información sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar a personas no autorizadas, estableciendo medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, de forma que se facilite a los ciudadanos y a las administraciones públicas el ejercicio de sus derechos y el cumplimiento de sus obligaciones a través de medios electrónicos.

Desde 2010 se han producido notables cambios en España y en la Unión Europea, incluidos la progresiva transformación digital de nuestra sociedad, el nuevo escenario de la ciberseguridad y el avance de las tecnologías de aplicación. Asimismo, se ha evidenciado que los sistemas de información están expuestos de forma cada vez más intensa a la materialización de amenazas del ciberespacio, advirtiéndose un notable incremento de los ciberataques, tanto en volumen y frecuencia como en sofisticación, con agentes y actores con mayores capacidades técnicas y operativas; amenazas que se producen en un contexto de alta dependencia de las tecnologías de la información y de las comunicaciones en nuestra sociedad y de gran interconexión de los sistemas de información. Todo ello afecta significativamente a un número cada vez mayor de entidades públicas y privadas, a sus cadenas de suministro, a los ciudadanos y, por ende, a la ciberseguridad nacional, lo que compromete el normal desenvolvimiento social y económico del país y el ejercicio de los derechos y libertades de los ciudadanos, como reconocen tanto la Estrategia de Ciberseguridad Nacional de 2013 como, particularmente, la Estrategia Nacional de Ciberseguridad 2019.

El Real Decreto 3/2010, de 8 de enero, establecía que el ENS debía desarrollarse y perfeccionarse manteniéndose actualizado de forma permanente conforme al progreso de los servicios de la administración electrónica, de la evolución de la tecnología, de los nuevos

estándares internacionales sobre seguridad y auditoría, y la consolidación de las infraestructuras que le sirven de apoyo.

En el plano normativo, acompasado a dichos cambios y en ocasiones como origen de los mismos, desde 2010 se han modificado tanto el marco europeo (con cuatro Reglamentos y una Directiva) como el español, referido a la seguridad nacional, regulación del procedimiento administrativo y el régimen jurídico del sector público, de protección de datos personales y de la seguridad de las redes y sistemas de información, y se ha evolucionado el marco estratégico de la ciberseguridad.

Así, la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, considera a la ciberseguridad como un ámbito de especial interés de la Seguridad Nacional tal como señala su artículo 10, y que, por ello, requiere una atención específica por resultar básica para preservar los derechos y libertades y el bienestar de los ciudadanos y para garantizar el suministro de los servicios y recursos esenciales. De acuerdo con las previsiones de su artículo 4.3 se aprobó el Real Decreto 1008/2017, de 1 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2017, y posteriormente, el Real Decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021, identificando en ambas al ciberespacio como un espacio común global, que la Estrategia 2021 describe como espacio de conexión caracterizado por su apertura funcional, la carencia de fronteras físicas y su fácil accesibilidad, añadiendo que en los espacios comunes globales resulta difícil la atribución de cualquier acción irregular o delictiva, dada su extensión, su débil regulación y la ausencia de soberanía.

Por otra parte, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, ha ampliado el ámbito de aplicación del ENS a todo el sector público, estableciendo en su artículo 3, que regula los principios generales, la necesidad de que las administraciones públicas se relacionen entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos, que garanticen la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas y la protección de los datos personales, y faciliten la prestación de servicios a los interesados preferentemente por dichos medios, señalando al ENS como instrumento fundamental para el logro de dichos objetivos en su artículo 156.

Asimismo, la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, entre los derechos de las personas en sus relaciones con las administraciones públicas previstos en el artículo 13 incluye el relativo a la protección de los datos personales y, en particular, el derecho a la seguridad de los datos que figuren en los ficheros, sistemas y aplicaciones de las administraciones públicas.

En desarrollo de las dos leyes anteriores, el Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos, concreta en diferentes preceptos la obligación del cumplimiento de las medidas de seguridad previstas en el ENS, como los referidos al intercambio electrónico de datos en entornos cerrados de comunicación, los sistemas de clave concertada y otros sistemas de identificación de las personas interesadas, el archivo electrónico único o los portales de internet, entre otros.

Coincidente en el tiempo con la aprobación de las tres leyes mencionadas, el Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, actualizó el ENS a la luz de la experiencia y conocimiento en su aplicación, de la situación de la ciberseguridad del momento, y de la evolución del marco legal, para adecuarse a lo previsto en el Reglamento (UE) n.º 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE (conocido como «Reglamento eIDAS»).

Con relación a las medidas de seguridad del ENS en el tratamiento de datos personales, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, ordenó en su disposición adicional primera que dichas medidas de seguridad se implanten en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679, del

Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). De otra parte, la disposición adicional primera también prescribe la implantación de las medidas de seguridad del ENS a las entidades del sector público y a las del sector privado que colaboren con estas en la prestación de servicios públicos que involucren el tratamiento de datos personales. Por último, y en el mismo sentido, la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, ha establecido en su artículo 37 la obligación de aplicar las medidas del ENS a los tratamientos de datos personales por parte de las autoridades públicas competentes.

Por otra parte, con relación a la seguridad de redes y sistemas de información, desde la entrada en vigor del Real Decreto 3/2010, de 8 de enero, se han aprobado en la Unión Europea dos Reglamentos y una Directiva que han fijado el marco de actuación en los ordenamientos nacionales.

Así, en primer lugar, el Reglamento (UE) N.º 526/2013 del Parlamento Europeo y del Consejo de 21 de mayo de 2013 relativo a la Agencia de Seguridad de las Redes de la Información de la Unión Europea (ENISA) y por el que se deroga el Reglamento (CE) N.º 460/2004. En segundo lugar, el Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.º 526/2013 («Reglamento sobre la Ciberseguridad»).

En tercer lugar, la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, conocida como «Directiva NIS (*Security of Network and Information Systems)*», que ha sido objeto de transposición en España por medio del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, señalando la necesidad de tener en cuenta el ENS en el momento de elaborar las disposiciones reglamentarias, instrucciones y guías, y adoptar las medidas aplicables a entidades del ámbito de aplicación de este. Este Real Decreto-ley 12/2018, de 7 de septiembre, ha sido desarrollado por el Real Decreto 43/2021, de 26 de enero, en lo relativo al marco estratégico e institucional de seguridad de las redes y sistemas de información, la supervisión del cumplimiento de las obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales, y la gestión de incidentes de seguridad. Así, el Real Decreto 43/2021, de 26 de enero, establece que las medidas para el cumplimiento de las obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales tomarán como referencia las recogidas en el anexo II del Real Decreto 3/2010, de 8 de enero.

Tal como estableció la Estrategia de Seguridad Nacional de 2017, España precisa garantizar un uso seguro y responsable de las redes y sistemas de información y comunicaciones a través del fortalecimiento de las capacidades de prevención, detección y respuesta a los ciberataques potenciando y adoptando medidas específicas para contribuir a la promoción de un ciberespacio seguro y fiable. En este sentido, el Consejo de Seguridad Nacional aprobó el 12 de abril de 2019 la Estrategia Nacional de Ciberseguridad 2019, publicada por Orden PCI/487/2019, de 26 de abril, con el propósito de fijar las directrices generales en el ámbito de la ciberseguridad de manera que se alcanzasen los objetivos previstos en la Estrategia de Seguridad Nacional de 2017.

La Estrategia Nacional de Ciberseguridad 2019, contiene un objetivo general y cinco objetivos específicos, y, para alcanzarlos, se proponen siete líneas de acción con un total de 65 medidas. El primero de estos objetivos es la seguridad y resiliencia de las redes y sistemas de información y comunicaciones del sector público y de los servicios esenciales y se desarrolla a través de dos líneas de acción y veinticuatro medidas específicas entre las que figura la de asegurar la plena implantación del Esquema Nacional de Seguridad. Para desarrollar esta Estrategia, el Consejo de Ministros ha aprobado el 29 de marzo de 2022 el

Plan Nacional de Ciberseguridad, que prevé cerca de 150 iniciativas, entre actuaciones y proyectos, para los próximos tres años.

Asimismo, la Estrategia Nacional de Ciberseguridad 2019 señala entre sus objetivos la consolidación de un marco nacional coherente e integrado que garantice la protección de la información y de los datos personales tratados por los sistemas y redes del sector público y de los servicios, sean o no esenciales, recogiendo que su cumplimiento requiere la implantación de medidas de seguridad enfocadas a mejorar las capacidades de prevención, detección y respuesta ante incidentes, mediante el desarrollo de nuevas soluciones, y el refuerzo de la coordinación y la adaptación del ordenamiento jurídico.

II

La evolución de las amenazas, los nuevos vectores de ataque, el desarrollo de modernos mecanismos de respuesta y la necesidad de mantener la conformidad y el alineamiento con las regulaciones europeas y nacionales de aplicación, exigen adaptar las medidas de seguridad a esta nueva realidad. Fortalecer la ciberseguridad demanda recursos económicos, humanos y tecnológicos que se han de dimensionar atendiendo al principio de proporcionalidad y al nivel de seguridad requerido, de acuerdo con una adecuada planificación y contando con la participación de los agentes involucrados, según una dinámica de mejora continua adaptativa.

Por ello, en un mundo hiperconectado como el actual, implementar la seguridad en el ciberespacio se ha convertido en una prioridad estratégica. Sin embargo, el riesgo en el ciberespacio es demasiado grande para que el sector público o las empresas lo aborden por sí solos, pues ambos comparten el interés y la responsabilidad de enfrentar juntos ese reto. A medida que aumenta el papel de la tecnología en la sociedad, la ciberseguridad se convierte en un desafío cada vez mayor.

De hecho, el pasado 9 de marzo, el Parlamento Europeo ha aprobado por amplísima mayoría una Resolución sobre injerencias extranjeras en todos los procesos democráticos de la Unión Europea, en particular la desinformación. Tal como señala dicha Resolución en sus considerandos, las injerencias extranjeras constituyen un patrón de conducta que amenaza o afecta negativamente a valores, procedimientos democráticos, procesos políticos, la seguridad de Estados y ciudadanos y la capacidad de hacer frente a situaciones excepcionales. Las tácticas de injerencia extranjera, que se combinan a menudo para tener un mayor efecto, adoptan, entre otras formas, los ciberataques, la asunción del control de infraestructuras críticas, la desinformación, supresión de información, manipulación de plataformas de redes sociales y de sus algoritmos, operaciones de pirateo y filtración, amenazas y acoso para acceder a información sobre los votantes e interferir en la legitimidad del proceso electoral, personalidades e identidades falsas, ejercicio de presiones sobre ciudadanos extranjeros que viven en la Unión, instrumentalización de migrantes y espionaje.

Al tiempo que el escenario descrito ha venido consolidándose, se ha ido extendiendo la implantación del ENS, resultando de ello una mayor experiencia acumulada sobre su aplicación, a la vez que un mejor conocimiento de la situación gracias a las sucesivas ediciones del Informe Nacional del Estado de la Seguridad (INES), del cuerpo de guías de seguridad CCN-STIC y de los servicios y herramientas proporcionados por la capacidad de respuesta a incidentes de seguridad de la información, el CCN-CERT, del Centro Criptológico Nacional (CCN).

En definitiva, por todas las razones anteriormente expuestas es necesario actualizar el ENS para cumplir tres grandes objetivos.

En primer lugar, alinear el ENS con el marco normativo y el contexto estratégico existente para garantizar la seguridad en la administración digital. Se trata de reflejar con claridad el ámbito de aplicación del ENS en beneficio de la ciberseguridad y de los derechos de los ciudadanos, así como de actualizar las referencias al marco legal vigente y de revisar la formulación de ciertas cuestiones a la luz de éste, conforme a la Estrategia Nacional de Ciberseguridad 2019 y el Plan Nacional de Ciberseguridad, de forma que se logre simplificar, precisar o armonizar los mandatos del ENS, eliminar aspectos que puedan considerarse excesivos, o añadir aquellos otros que se identifican como necesarios.

En segundo lugar, introducir la capacidad de ajustar los requisitos del ENS, para garantizar su adaptación a la realidad de ciertos colectivos o tipos de sistemas, atendiendo a la semejanza que presentan una multiplicidad de entidades o servicios en cuanto a los riesgos a los que están expuestos sus sistemas de información y sus servicios. Ello aconseja la inclusión en el ENS del concepto de «perfil de cumplimiento específico» que, aprobado por el Centro Criptológico Nacional, permita alcanzar una adaptación del ENS más eficaz y eficiente, racionalizando los recursos requeridos sin menoscabo de la protección perseguida y exigible.

En tercer lugar, facilitar una mejor respuesta a las tendencias en ciberseguridad, reducir vulnerabilidades y promover la vigilancia continua mediante la revisión de los principios básicos, de los requisitos mínimos y de las medidas de seguridad.

Por último, la aprobación de este real decreto se incardina también en la ejecución del Plan de Digitalización de las Administraciones Públicas 2021-2025, uno de los instrumentos principales para el cumplimiento del Plan de Recuperación, Transformación y Resiliencia y su Componente 11 denominado «Modernización de las Administraciones Públicas», así como para el desarrollo de las inversiones y reformas previstas en la agenda España Digital 2025. Dicho Plan de Digitalización contempla expresamente, entre sus reformas, la actualización del ENS con el fin de hacer evolucionar la política de seguridad de todas las entidades del sector público español, tomando en cuenta las regulaciones de la Unión Europea dirigidas a incrementar el nivel de ciberseguridad de los sistemas de información. Dicha reforma se ve complementada con la constitución del Centro de Operaciones de Ciberseguridad de la Administración General del Estado y sus Organismos Públicos que servirá de referencia para las demás administraciones públicas y contribuirá a mejorar el cumplimiento del ENS de las entidades en su alcance de servicio. Esta previsión ha sido respaldada por el Acuerdo de Consejo de Ministros de 25 de mayo de 2021 sobre actuaciones urgentes en materia de ciberseguridad que mandata la tramitación y aprobación de un real decreto que sustituya al Real Decreto 3/2010, de 8 de enero, como medida de refuerzo del marco normativo.

III

El real decreto se estructura en cuarenta y un artículos distribuidos en siete capítulos, tres disposiciones adicionales, una disposición transitoria, una disposición derogatoria, tres disposiciones finales y cuatro anexos.

El capítulo I comprende las disposiciones generales que regulan el objeto de la norma, su ámbito de aplicación, la referencia a los sistemas de información que traten datos personales y las definiciones aplicables. El ámbito de aplicación es el previsto en el artículo 2 de la Ley 40/2015, de 1 de octubre, al que se añaden los sistemas que tratan información clasificada, sin perjuicio de la normativa que resulte de aplicación, pudiendo resultar necesario complementar las medidas de seguridad de este real decreto con otras específicas para tales sistemas, derivadas de los compromisos internacionales contraídos por España o su pertenencia a organismos o foros internacionales en la materia. Asimismo los requisitos del ENS serán de aplicación a los sistemas de información de las entidades del sector privado, cuando de acuerdo con la normativa aplicable y en virtud de una relación contractual presten servicios a las entidades del sector público para el ejercicio por estas de sus competencias y potestades administrativas. Como se ha señalado anteriormente, considerando que la transformación digital ha supuesto un incremento de los riesgos asociados a los sistemas de información que sustentan los servicios públicos y que el sector privado se encuentra igualmente inmerso en la transformación digital de sus procesos de negocio, ambos tipos de sistemas de información se encuentran expuestos al mismo tipo de amenazas y riesgos. Por ello, los operadores del sector privado que prestan servicios a las entidades del sector público, por razón de la alta imbricación de unos y otras, han de garantizar el mismo nivel de seguridad que se aplica a los sistemas y a la información en el ámbito del sector público, todo ello de conformidad, además, con los especiales requerimientos establecidos tanto en la Ley Orgánica 3/2018, de 5 de diciembre, como en la Ley Orgánica 7/2021, de 26 de mayo. Por otra parte, cuando las entidades del sector público lleven a cabo la instalación, despliegue y explotación de redes 5G o la prestación de servicios 5G, además de las previsiones de este real decreto será de aplicación lo

establecido en el Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación, en particular, lo dispuesto en su artículo 17 relativo a la gestión de seguridad por las administraciones públicas, así como su normativa de desarrollo.

El capítulo II, que comprende los artículos 5 a 11, regula los principios básicos que deben regir el ENS y que enumera en su artículo 5: seguridad integral; gestión de la seguridad basada en los riesgos; prevención, detección, respuesta y conservación; existencia de líneas de defensa; vigilancia continua y reevaluación periódica; y diferenciación de responsabilidades.

El capítulo III se refiere a la Política de Seguridad y los requisitos mínimos para permitir una protección adecuada de la información y los servicios. En los artículos 12 a 27 se definen tales requisitos: organización e implantación del proceso de seguridad; gestión de riesgos, consistente en un proceso de identificación, análisis, evaluación y tratamiento de los mismos; gestión de personal; profesionalidad; autorización y control de los accesos; protección de las instalaciones; adquisición de productos de seguridad y contratación de servicios de seguridad; mínimo privilegio; integridad y actualización del sistema; protección de la información almacenada y en tránsito; prevención ante otros sistemas de información interconectados; registro de la actividad y detección de código dañino; incidentes de seguridad; continuidad de la actividad; y mejora continua del proceso de seguridad. Seguidamente, el artículo 28 indica que para el cumplimiento de tales requisitos mínimos deberán adoptarse las medidas recogidas en el anexo II, conforme a una serie de consideraciones al efecto. No obstante, tales medidas de seguridad podrán ser reemplazadas por otras compensatorias, siempre y cuando se justifique documentalmente que la protección que aportan es, al menos, equivalente, y satisfacen los principios básicos y requisitos mínimos indicados previamente. En el artículo 29 se hace un llamamiento a la utilización de infraestructuras y servicios comunes de las administraciones públicas en aras de lograr una mayor eficiencia y retroalimentación de las sinergias de cada colectivo. Por último, el artículo 30 establece la posibilidad de implementar perfiles de cumplimiento específicos, así como esquemas de acreditación de entidades de implementación de configuraciones seguras.

El capítulo IV versa sobre la auditoría de la seguridad, el informe del estado de la seguridad y la respuesta a incidentes de seguridad. La auditoría de la seguridad se desarrolla íntegramente en el artículo 31, detallando las características del procedimiento de auditoría, así como de los correspondientes informes. Por su parte, el artículo 32, relativo al informe del estado de la seguridad, destaca el papel de la Comisión Sectorial de Administración Electrónica en este ámbito, así como del CCN y los órganos colegiados competentes en el ámbito de la administración digital en la Administración General del Estado.

La prevención, detección y respuesta a incidentes de seguridad se regula en los artículos 33 y 34, separando, por un lado, los aspectos relativos a la capacidad de respuesta y, por otro, los relativo a la prestación de los servicios de respuesta a incidentes de seguridad, tanto a las entidades del Sector Público como a las organizaciones del sector privado que les presten servicios.

En el capítulo V, artículos 35 a 38, se definen las normas de conformidad, que se concretan en cuatro: Administración Digital, ciclo de vida de servicios y sistemas, mecanismos de control y procedimientos de determinación de la conformidad con el ENS.

Por su parte, el capítulo VI, compuesto por su único artículo, el 39, establece la obligación de actualización permanente, de acuerdo con el marco jurídico vigente en cada momento, la evolución de la tecnología y los estándares en materia de seguridad y sistemas, así como de las ya mencionadas nuevas amenazas y vectores de ataque.

Concluye el articulado de la parte dispositiva con el capítulo VII, que desarrolla el procedimiento de categorización de los sistemas de información, definiendo en el artículo 40 las categorías de seguridad y en el artículo 41 las facultades al respecto.

En cuanto a las tres disposiciones adicionales, la primera regula los programas de sensibilización, concienciación y formación, dirigidos al personal de las entidades del sector público que desarrollarán el CCN y el Instituto Nacional de Administración Pública.

La segunda disposición adicional regula las instrucciones técnicas de seguridad, de obligado cumplimiento y las guías de seguridad de las tecnologías de la información y la comunicación (guías CCN-STIC).

Por último, la tercera disposición adicional establece el cumplimiento del llamado principio de «no causar un perjuicio significativo» al medioambiente (principio DNSH, por sus siglas en inglés, *Do No Significant Harm)* y las condiciones del etiquetado climático y digital.

La disposición transitoria única fija un plazo de veinticuatro meses para que los sistemas de información del ámbito de aplicación de este real decreto, preexistentes a su entrada en vigor, alcancen su plena adecuación al ENS.

La disposición derogatoria suprime el Real Decreto 3/2010, de 8 de enero, así como cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en este real decreto.

Por último, la norma cuenta con tres disposiciones finales. La primera de ellas enumera los títulos competenciales; la segunda disposición final habilita a la persona titular del Ministerio de Asuntos Económicos y Transformación Digital para dictar las disposiciones necesarias para la su aplicación y desarrollo, sin perjuicio de las competencias de las comunidades autónomas para el desarrollo y ejecución de la legislación básica del Estado, y la disposición final tercera ordena la entrada en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

El real decreto se complementa con cuatro anexos: el anexo I regula las categorías de seguridad de los sistemas de información, detallando la secuencia de actuaciones para determinar la categoría de seguridad de un sistema; el anexo II detalla las medidas de seguridad; el anexo III se ocupa del objeto, niveles e interpretación de la Auditoría de la seguridad y, por último, el anexo IV incluye el glosario de términos y definiciones.

Con relación, en particular, al anexo II, este detalla las medidas de seguridad estructuradas en tres grupos: el marco organizativo, constituido por el conjunto de medidas relacionadas con la organización global de la seguridad; el marco operacional, formado por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin; y las medidas de protección, que se centran en proteger activos concretos, según su naturaleza y la calidad exigida por el nivel de seguridad de las dimensiones afectadas. Como se ha dicho, la modificación del marco táctico y operativo en el que se desenvuelven las ciberamenazas y sus correlativas salvaguardas ha obligado a actualizar el elenco de medidas de seguridad del anexo II, con objeto de añadir, eliminar o modificar controles y sub-controles, al tiempo que se incluye un nuevo sistema de referencias más moderno y adecuado, sobre la base de la existencia de un requisito general y de unos posibles refuerzos, alineados con el nivel de seguridad perseguido. Todo ello se efectúa con el objetivo de afianzar de manera proporcionada la seguridad de los sistemas de información concernidos, y facilitar su implantación y auditoría.

IV

El real decreto, cuya aprobación está incluida en el Plan Anual Normativo de la Administración General del Estado para el año 2022, se ajusta a los principios de buena regulación contenidos en el artículo 129 de la Ley 39/2015, de 1 de octubre (principios de necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia y eficiencia).

Así, la norma es acorde con los principios de necesidad y eficacia en tanto que persigue un interés general al concretar la regulación del ENS desarrollando en este aspecto la Ley 40/2015, de 1 de octubre y otros aspectos concretos de la normativa nacional y de la Unión Europea mencionada en este preámbulo. La norma es también acorde con el principio de proporcionalidad, al contener la regulación imprescindible para la consecución de los objetivos previamente mencionados. Igualmente, se ajusta al principio de seguridad jurídica, siendo coherente con el resto del ordenamiento, estableciéndose un marco normativo estable, integrado y claro. Durante el procedimiento de elaboración de la norma y aún en el contexto de la aplicación de las previsiones del artículo 27 de la Ley 50/1997, de 27 de noviembre, del Gobierno, por tratarse de una tramitación de urgencia acordada por el Consejo de Ministros, se han formalizado los trámites de audiencia e información pública, conforme a lo previsto en el artículo 133 de la Ley 39/2015, de 1 de octubre, y el artículo 26 de la Ley 50/1997, de 27 de noviembre, en cumplimiento del principio de transparencia,

quedando además justificados en el preámbulo los objetivos que persigue este real decreto. El proyecto se ha sometido a consulta a las comunidades autónomas y a la Federación Española de Municipios y Provincias a través de la Comisión Sectorial de Administración Electrónica y ha sido informado por la Comisión Nacional de los Mercados y la Competencia A.A.I. y la Agencia Española de Protección de Datos A.A.I.

Por último, en virtud del principio de eficiencia la norma no introduce ninguna variación en materia de cargas administrativas, respecto de la normativa que desarrolla.

El real decreto se aprueba en ejercicio de las competencias previstas en los artículos 149.1.18.ª, 149.1.21.ª y 149.1.29.ª de la Constitución, que atribuyen al Estado la competencia exclusiva sobre las bases del régimen jurídico de las administraciones públicas, sobre las telecomunicaciones y sobre la seguridad pública, respectivamente.

En su virtud, a propuesta de la Ministra de Asuntos Económicos y Transformación Digital, con la aprobación previa de la Ministra de Hacienda y Función Pública, de acuerdo con el Consejo de Estado, y previa deliberación del Consejo de Ministros en su reunión del día 3 de mayo de 2022,

DISPONGO:

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

1. Este real decreto tiene por objeto regular el Esquema Nacional de Seguridad (en adelante, ENS), establecido en el artículo 156.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

2. El ENS está constituido por los principios básicos y requisitos mínimos necesarios para una protección adecuada de la información tratada y los servicios prestados por las entidades de su ámbito de aplicación, con objeto de asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos que gestionen en el ejercicio de sus competencias.

3. Lo dispuesto en este real decreto, por cuanto afecta a los sistemas de información utilizados para la prestación de los servicios públicos, deberá considerarse comprendido en los recursos y procedimientos integrantes del Sistema de Seguridad Nacional recogidos en la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.

Artículo 2. *Ámbito de aplicación.*

1. El presente real decreto es de aplicación a todo el sector público, en los términos en que este se define por el artículo 2 de la Ley 40/2015, de 1 de octubre, y de acuerdo con lo previsto en el artículo 156.2 de la misma.

2. Asimismo, sin perjuicio de la aplicación de la Ley 9/1968, de 5 de abril, de Secretos Oficiales y otra normativa especial, este real decreto será de aplicación a los sistemas que tratan información clasificada, pudiendo resultar necesario adoptar medidas complementarias de seguridad, específicas para dichos sistemas, derivadas de los compromisos internacionales contraídos por España o de su pertenencia a organismos o foros internacionales.

3. Este real decreto también se aplica a los sistemas de información de las entidades del sector privado, incluida la obligación de contar con la política de seguridad a que se refiere el artículo 12, cuando, de acuerdo con la normativa aplicable y en virtud de una relación contractual, presten servicios o provean soluciones a las entidades del sector público para el ejercicio por estas de sus competencias y potestades administrativas.

La política de seguridad a que se refiere el artículo 12 será aprobada en el caso de estas entidades por el órgano que ostente las máximas competencias ejecutivas.

Los pliegos de prescripciones administrativas o técnicas de los contratos que celebren las entidades del sector público incluidas en el ámbito de aplicación de este real decreto

contemplarán todos aquellos requisitos necesarios para asegurar la conformidad con el ENS de los sistemas de información en los que se sustenten los servicios prestados por los contratistas, tales como la presentación de las correspondientes Declaraciones o Certificaciones de Conformidad con el ENS.

Esta cautela se extenderá también a la cadena de suministro de dichos contratistas, en la medida que sea necesario y de acuerdo con los resultados del correspondiente análisis de riesgos.

4. Cuando las entidades del sector público lleven a cabo la instalación, despliegue y explotación de redes 5G o la prestación de servicios 5G, además de las previsiones de este real decreto será de aplicación lo establecido en el Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación, en particular, lo dispuesto en su artículo 17 relativo a la gestión de seguridad por las administraciones públicas, así como su normativa de desarrollo.

Artículo 3. *Sistemas de información que traten datos personales.*

1. Cuando un sistema de información trate datos personales le será de aplicación lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos) y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, o, en su caso, la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, el resto de normativa de aplicación, así como los criterios que se establezcan por la Agencia Española de Protección de Datos o en su ámbito competencial, por las autoridades autonómicas de protección de datos, sin perjuicio de los requisitos establecidos en el presente real decreto.

2. En estos supuestos, el responsable o el encargado del tratamiento, asesorado por el delegado de protección de datos, realizarán un análisis de riesgos conforme al artículo 24 del Reglamento General de Protección de Datos y, en los supuestos de su artículo 35, una evaluación de impacto en la protección de datos.

3. En todo caso, prevalecerán las medidas a implantar como consecuencia del análisis de riesgos y, en su caso, de la evaluación de impacto a los que se refiere el apartado anterior, en caso de resultar agravadas respecto de las previstas en el presente real decreto.

Artículo 4. *Definiciones.*

A los efectos previstos en este real decreto, las definiciones, palabras, expresiones y términos han de ser entendidos en el sentido indicado en el Glosario de términos incluido en el anexo IV.

CAPÍTULO II

Principios básicos

Artículo 5. *Principios básicos del Esquema Nacional de Seguridad.*

El objeto último de la seguridad de la información es garantizar que una organización podrá cumplir sus objetivos, desarrollar sus funciones y ejercer sus competencias utilizando sistemas de información. Por ello, en materia de seguridad de la información deberán tenerse en cuenta los siguientes principios básicos:

a) Seguridad como proceso integral.
b) Gestión de la seguridad basada en los riesgos.
c) Prevención, detección, respuesta y conservación.
d) Existencia de líneas de defensa.
e) Vigilancia continua.
f) Reevaluación periódica.
g) Diferenciación de responsabilidades.

Artículo 6. *La seguridad como un proceso integral.*

1. La seguridad se entiende como un proceso integral constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con el sistema de información. La aplicación del ENS estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.

2. Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y la de los responsables jerárquicos, para evitar que, la ignorancia, la falta de organización y de coordinación o de instrucciones adecuadas, constituyan fuentes de riesgo para la seguridad.

Artículo 7. *Gestión de la seguridad basada en los riesgos.*

1. El análisis y la gestión de los riesgos es parte esencial del proceso de seguridad, debiendo constituir una actividad continua y permanentemente actualizada.

2. La gestión de los riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos a niveles aceptables. La reducción a estos niveles se realizará mediante una apropiada aplicación de medidas de seguridad, de manera equilibrada y proporcionada a la naturaleza de la información tratada, de los servicios a prestar y de los riesgos a los que estén expuestos.

Artículo 8. *Prevención, detección, respuesta y conservación.*

1. La seguridad del sistema debe contemplar las acciones relativas a los aspectos de prevención, detección y respuesta, al objeto de minimizar sus vulnerabilidades y lograr que las amenazas sobre el mismo no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información que maneja o a los servicios que presta.

2. Las medidas de prevención, que podrán incorporar componentes orientados a la disuasión o a la reducción de la superficie de exposición, deben eliminar o reducir la posibilidad de que las amenazas lleguen a materializarse.

3. Las medidas de detección irán dirigidas a descubrir la presencia de un ciberincidente.

4. Las medidas de respuesta, que se gestionarán en tiempo oportuno, estarán orientadas a la restauración de la información y los servicios que pudieran haberse visto afectados por un incidente de seguridad.

5. Sin merma de los restantes principios básicos y requisitos mínimos establecidos, el sistema de información garantizará la conservación de los datos e información en soporte electrónico.

De igual modo, el sistema mantendrá disponibles los servicios durante todo el ciclo vital de la información digital, a través de una concepción y procedimientos que sean la base para la preservación del patrimonio digital.

Artículo 9. *Existencia de líneas de defensa.*

1. El sistema de información ha de disponer de una estrategia de protección constituida por múltiples capas de seguridad, dispuesta de forma que, cuando una de las capas sea comprometida, permita:

a) Desarrollar una reacción adecuada frente a los incidentes que no han podido evitarse, reduciendo la probabilidad de que el sistema sea comprometido en su conjunto.

b) Minimizar el impacto final sobre el mismo.

2. Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, física y lógica.

Artículo 10. *Vigilancia continua y reevaluación periódica.*

1. La vigilancia continua permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta.

2. La evaluación permanente del estado de la seguridad de los activos permitirá medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.

3. Las medidas de seguridad se reevaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.

Artículo 11. *Diferenciación de responsabilidades.*

1. En los sistemas de información se diferenciará el responsable de la información, el responsable del servicio, el responsable de la seguridad y el responsable del sistema.
2. La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la explotación de los sistemas de información concernidos.
3. La política de seguridad de la organización detallará las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos.

CAPÍTULO III

Política de seguridad y requisitos mínimos de seguridad

Artículo 12. *Política de seguridad y requisitos mínimos de seguridad.*

1. La política de seguridad de la información es el conjunto de directrices que rigen la forma en que una organización gestiona y protege la información que trata y los servicios que presta. A tal efecto, el instrumento que apruebe dicha política de seguridad deberá incluir, como mínimo, los siguientes extremos:

a) Los objetivos o misión de la organización.
b) El marco regulatorio en el que se desarrollarán las actividades.
c) Los roles o funciones de seguridad, definiendo para cada uno, sus deberes y responsabilidades, así como el procedimiento para su designación y renovación.
d) La estructura y composición del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad y la relación con otros elementos de la organización.
e) Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.
f) Los riesgos que se derivan del tratamiento de los datos personales.

2. Cada administración pública contará con una política de seguridad formalmente aprobada por el órgano competente. Asimismo, cada órgano o entidad con personalidad jurídica propia comprendido en el ámbito subjetivo del artículo 2 deberá contar con una política de seguridad formalmente aprobada por el órgano competente.
No obstante, la totalidad o una parte de los sujetos de un sector público institucional podrán quedar incluidos en el ámbito subjetivo de la política de seguridad aprobada por la Administración con la que guarden relación de vinculación, dependencia o adscripción, cuando así lo determinen los órganos competentes en el ejercicio de las potestades de organización.
3. En la Administración General del Estado, cada ministerio contará con su política de seguridad, que aprobará la persona titular del Departamento. Los organismos públicos y entidades pertenecientes al sector público institucional estatal podrán contar con su propia política de seguridad, aprobada por el órgano competente, que será coherente con la del Departamento con el que mantenga la relación de vinculación, dependencia o adscripción, o bien quedar comprendidos en el ámbito subjetivo de la política de seguridad de este. También podrán contar con su propia política de seguridad, aprobada por el órgano competente, coherente con la del Departamento del que dependan o al que estén adscritos, los centros directivos de la propia Administración General del Estado que gestionen servicios bajo la declaración de servicios compartidos.
4. La Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital dispondrá de su propia política de seguridad, que será aprobada por la persona titular de la misma.
5. Los municipios podrán disponer de una política de seguridad común elaborada por la entidad local comarcal o provincial que asuma la responsabilidad de la seguridad de la información de los sistemas municipales.

6. La política de seguridad se establecerá de acuerdo con los principios básicos señalados en el capítulo II y se desarrollará aplicando los siguientes requisitos mínimos:

a) Organización e implantación del proceso de seguridad.
b) Análisis y gestión de los riesgos.
c) Gestión de personal.
d) Profesionalidad.
e) Autorización y control de los accesos.
f) Protección de las instalaciones.
g) Adquisición de productos de seguridad y contratación de servicios de seguridad.
h) Mínimo privilegio.
i) Integridad y actualización del sistema.
j) Protección de la información almacenada y en tránsito.
k) Prevención ante otros sistemas de información interconectados.
l) Registro de la actividad y detección de código dañino.
m) Incidentes de seguridad.
n) Continuidad de la actividad.
ñ) Mejora continua del proceso de seguridad.

7. Los requisitos mínimos se exigirán en proporción a los riesgos identificados en cada sistema, de conformidad con lo dispuesto en el artículo 28, alguno de los cuales podrá obviarse en sistemas sin riesgos significativos.

Artículo 13. *Organización e implantación del proceso de seguridad.*

1. La seguridad de los sistemas de información deberá comprometer a todos los miembros de la organización.
2. La política de seguridad, en aplicación del principio de diferenciación de responsabilidades a que se refiere el artículo 11 y según se detalla en la sección 3.1 del anexo II, deberá ser conocida por todas las personas que formen parte de la organización e identificar de forma inequívoca a los responsables de velar por su cumplimiento, los cuales tendrán las siguientes funciones:

a) El responsable de la información determinará los requisitos de la información tratada
b) El responsable del servicio determinará los requisitos de los servicios prestados.
c) El responsable de la seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones.
d) El responsable del sistema, por sí o a través de recursos propios o contratados, se encargará de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad.

3. El responsable de la seguridad será distinto del responsable del sistema, no debiendo existir dependencia jerárquica entre ambos. En aquellas situaciones excepcionales en las que la ausencia justificada de recursos haga necesario que ambas funciones recaigan en la misma persona o en distintas personas entre las que exista relación jerárquica, deberán aplicarse medidas compensatorias para garantizar la finalidad del principio de diferenciación de responsabilidades previsto en el artículo 11.
4. Una Instrucción Técnica de Seguridad regulará el Esquema de Certificación de Responsables de la Seguridad, que recogerá las condiciones y requisitos exigibles a esta figura.
5. En el caso de servicios externalizados, salvo por causa justificada y documentada, la organización prestataria de dichos servicios deberá designar un POC (Punto o Persona de Contacto) para la seguridad de la información tratada y el servicio prestado, que cuente con el apoyo de los órganos de dirección, y que canalice y supervise, tanto el cumplimiento de los requisitos de seguridad del servicio que presta o solución que provea, como las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dicho servicio.

Dicho POC de seguridad será el propio Responsable de Seguridad de la organización contratada, formará parte de su área o tendrá comunicación directa con la misma. Todo ello sin perjuicio de que la responsabilidad última resida en la entidad del sector público destinataria de los citados servicios.

Artículo 14. *Análisis y gestión de los riesgos.*

1. Cada organización que desarrolle e implante sistemas para el tratamiento de la información o la prestación de servicios realizará su propia gestión de riesgos.
2. Esta gestión se realizará por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema. Sin perjuicio de lo dispuesto en el anexo II, se empleará alguna metodología reconocida internacionalmente.
3. Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.

Artículo 15. *Gestión de personal.*

1. El personal, propio o ajeno, relacionado con los sistemas de información sujetos a lo dispuesto en este real decreto, deberá ser formado e informado de sus deberes, obligaciones y responsabilidades en materia de seguridad. Su actuación, que deberá ser supervisada para verificar que se siguen los procedimientos establecidos, aplicará las normas y procedimientos operativos de seguridad aprobados en el desempeño de sus cometidos.
2. El significado y alcance del uso seguro del sistema se concretará y plasmará en unas normas de seguridad que serán aprobadas por la dirección o el órgano superior correspondiente.

Artículo 16. *Profesionalidad.*

1. La seguridad de los sistemas de información estará atendida y será revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: planificación, diseño, adquisición, construcción, despliegue, explotación, mantenimiento, gestión de incidencias y desmantelamiento.
2. Las entidades del ámbito de aplicación de este real decreto exigirán, de manera objetiva y no discriminatoria, que las organizaciones que les presten servicios de seguridad cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados.
3. Las organizaciones determinarán los requisitos de formación y experiencia necesaria del personal para el desarrollo de su puesto de trabajo.

Artículo 17. *Autorización y control de los accesos.*

El acceso controlado a los sistemas de información comprendidos en el ámbito de aplicación de este real decreto deberá estar limitado a los usuarios, procesos, dispositivos u otros sistemas de información, debidamente autorizados, y exclusivamente a las funciones permitidas.

Artículo 18. *Protección de las instalaciones.*

Los sistemas de información y su infraestructura de comunicaciones asociada deberán permanecer en áreas controladas y disponer de los mecanismos de acceso adecuados y proporcionales en función del análisis de riesgos, sin perjuicio de lo establecido en la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas y en el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

Artículo 19. *Adquisición de productos de seguridad y contratación de servicios de seguridad.*

1. En la adquisición de productos de seguridad o contratación de servicios de seguridad de las tecnologías de la información y la comunicación que vayan a ser empleados en los

sistemas de información del ámbito de aplicación de este real decreto, se utilizarán, de forma proporcionada a la categoría del sistema y el nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.

2. El Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información del Centro Criptológico Nacional (en adelante, CCN), constituido al amparo de lo dispuesto en el artículo 2.2.c) del Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional, teniendo en cuenta los criterios y metodologías de evaluación nacionales e internacionales reconocidas por este organismo y en función del uso previsto del producto o servicio concreto dentro de sus competencias, determinará los siguientes aspectos:

a) Los requisitos funcionales de seguridad y de aseguramiento de la certificación.

b) Otras certificaciones de seguridad adicionales que se requieran normativamente.

c) Excepcionalmente, el criterio a seguir en los casos en que no existan productos o servicios certificados.

3. Para la contratación de servicios de seguridad se estará a lo señalado en los apartados anteriores y a lo dispuesto en el artículo 16.

Artículo 20. *Mínimo privilegio.*

Los sistemas de información deben diseñarse y configurarse otorgando los mínimos privilegios necesarios para su correcto desempeño, lo que implica incorporar los siguientes aspectos:

a) El sistema proporcionará la funcionalidad imprescindible para que la organización alcance sus objetivos competenciales o contractuales.

b) Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son desarrolladas por las personas autorizadas, desde emplazamientos o equipos asimismo autorizados; pudiendo exigirse, en su caso, restricciones de horario y puntos de acceso facultados.

c) Se eliminarán o desactivarán, mediante el control de la configuración, las funciones que sean innecesarias o inadecuadas al fin que se persigue. El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

d) Se aplicarán guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema, al efecto de eliminar o desactivar las funciones que sean innecesarias o inadecuadas.

Artículo 21. *Integridad y actualización del sistema.*

1. La inclusión de cualquier elemento físico o lógico en el catálogo actualizado de activos del sistema, o su modificación, requerirá autorización formal previa.

2. La evaluación y monitorización permanentes permitirán adecuar el estado de seguridad de los sistemas atendiendo a las deficiencias de configuración, las vulnerabilidades identificadas y las actualizaciones que les afecten, así como la detección temprana de cualquier incidente que tenga lugar sobre los mismos.

Artículo 22. *Protección de información almacenada y en tránsito.*

1. En la organización e implantación de la seguridad se prestará especial atención a la información almacenada o en tránsito a través de los equipos o dispositivos portátiles o móviles, los dispositivos periféricos, los soportes de información y las comunicaciones sobre redes abiertas, que deberán analizarse especialmente para lograr una adecuada protección.

2. Se aplicarán procedimientos que garanticen la recuperación y conservación a largo plazo de los documentos electrónicos producidos por los sistemas de información comprendidos en el ámbito de aplicación de este real decreto, cuando ello sea exigible.

3. Toda información en soporte no electrónico que haya sido causa o consecuencia directa de la información electrónica a la que se refiere este real decreto, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello, se aplicarán las medidas que

correspondan a la naturaleza del soporte, de conformidad con las normas que resulten de aplicación.

Artículo 23. *Prevención ante otros sistemas de información interconectados.*

Se protegerá el perímetro del sistema de información, especialmente, si se conecta a redes públicas, tal y como se definen en la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, reforzándose las tareas de prevención, detección y respuesta a incidentes de seguridad.

En todo caso, se analizarán los riesgos derivados de la interconexión del sistema con otros sistemas y se controlará su punto de unión. Para la adecuada interconexión entre sistemas se estará a lo dispuesto en la Instrucción Técnica de Seguridad correspondiente.

Artículo 24. *Registro de actividad y detección de código dañino.*

1. Con el propósito de satisfacer el objeto de este real decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los usuarios, reteniendo la información estrictamente necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

2. Al objeto de preservar la seguridad de los sistemas de información, garantizando la rigurosa observancia de los principios de actuación de las Administraciones públicas, y de conformidad con lo dispuesto en el Reglamento General de Protección de Datos y el respeto a los principios de limitación de la finalidad, minimización de los datos y limitación del plazo de conservación allí enunciados, los sujetos comprendidos en el artículo 2 podrán, en la medida estrictamente necesaria y proporcionada, analizar las comunicaciones entrantes o salientes, y únicamente para los fines de seguridad de la información, de forma que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la distribución malintencionada de código dañino así como otros daños a las antedichas redes y sistemas de información.

3. Para corregir o, en su caso, exigir responsabilidades, cada usuario que acceda al sistema de información deberá estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado una determinada actividad.

Artículo 25. *Incidentes de seguridad.*

1. La entidad titular de los sistemas de información del ámbito de este real decreto dispondrá de procedimientos de gestión de incidentes de seguridad de acuerdo con lo previsto en el artículo 33, la Instrucción Técnica de Seguridad correspondiente y, en caso de tratarse de un operador de servicios esenciales o de un proveedor de servicios digitales, de acuerdo con lo previsto en el anexo del Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

2. Asimismo, se dispondrá de mecanismos de detección, criterios de clasificación, procedimientos de análisis y resolución, así como de los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.

Artículo 26. *Continuidad de la actividad.*

Los sistemas dispondrán de copias de seguridad y se establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales.

Artículo 27. *Mejora continua del proceso de seguridad.*

El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a la gestión de la seguridad de las tecnologías de la información.

Artículo 28. *Cumplimiento de los requisitos mínimos.*

1. Para dar cumplimiento a los requisitos mínimos establecidos en el presente real decreto, las entidades comprendidas en su ámbito de aplicación adoptarán las medidas y refuerzos de seguridad correspondientes indicados en el anexo II, teniendo en cuenta:

a) Los activos que constituyen los sistemas de información concernidos.
b) La categoría del sistema, según lo previsto en el artículo 40 y en el anexo I.
c) Las decisiones que se adopten para gestionar los riesgos identificados.

2. Las medidas a las que se refiere el apartado 1 tendrán la condición de mínimos exigibles, siendo ampliables a criterio del responsable de la seguridad, quien podrá incluir medidas adicionales, habida cuenta del estado de la tecnología, la naturaleza de la información tratada o los servicios prestados y los riesgos a que están expuestos los sistemas de información afectados. La relación de medidas de seguridad seleccionadas se formalizará en un documento denominado Declaración de Aplicabilidad, firmado por el responsable de la seguridad.

3. Las medidas de seguridad referenciadas en el anexo II podrán ser reemplazadas por otras compensatorias, siempre y cuando se justifique documentalmente que protegen, igual o mejor, del riesgo sobre los activos (anexo I) y se satisfacen los principios básicos y los requisitos mínimos previstos en los capítulos II y III. Como parte integral de la Declaración de Aplicabilidad se indicará, de forma detallada, la correspondencia entre las medidas compensatorias implantadas y las medidas del anexo II que compensan. El conjunto será objeto de la aprobación formal por parte del responsable de la seguridad. Una Guía CCN-STIC de las previstas en la disposición adicional segunda guiará en la selección de dichas medidas, así como su registro e inclusión en la Declaración de Aplicabilidad.

Artículo 29. *Infraestructuras y servicios comunes.*

La utilización de infraestructuras y servicios comunes de las administraciones públicas, incluidos los compartidos o transversales, facilitará el cumplimiento de lo dispuesto en este real decreto. Los supuestos concretos de utilización de estas infraestructuras y servicios serán determinados por cada administración pública.

Artículo 30. *Perfiles de cumplimiento específicos y acreditación de entidades de implementación de configuraciones seguras.*

1. En virtud del principio de proporcionalidad y buscando una eficaz y eficiente aplicación del ENS a determinadas entidades o sectores de actividad concretos, se podrán implementar perfiles de cumplimiento específicos que comprenderán aquel conjunto de medidas de seguridad que, trayendo causa del preceptivo análisis de riesgos, resulten idóneas para una concreta categoría de seguridad.

2. De forma análoga a lo dispuesto en el apartado anterior, para posibilitar la adecuada implantación y configuración de soluciones o plataformas suministradas por terceros, que vayan a ser usadas por las entidades comprendidas en el ámbito de aplicación de este real decreto, se podrán implementar esquemas de acreditación de entidades y validación de personas, que garanticen la seguridad de dichas soluciones o plataformas y la conformidad con lo dispuesto en este real decreto.

3. El CCN, en el ejercicio de sus competencias, validará y publicará los correspondientes perfiles de cumplimiento específicos que se definan y los antedichos esquemas de acreditación y validación, de acuerdo con las instrucciones técnicas de seguridad y guías de seguridad aprobadas conforme a lo previsto en la disposición adicional segunda.

4. Las correspondientes instrucciones técnicas de seguridad o, en su caso, las guías de Seguridad CCN-STIC, precisarán las condiciones a las que deberán sujetarse las implementaciones en modo local de productos, sistemas o servicios originariamente

prestados en la nube o en forma remota, así como las condiciones específicas para su evaluación y auditoría.

CAPÍTULO IV

Seguridad de los sistemas: auditoría, informe e incidentes de seguridad

Artículo 31. *Auditoría de la seguridad.*

1. Los sistemas de información comprendidos en el ámbito de aplicación de este real decreto serán objeto de una auditoría regular ordinaria, al menos cada dos años, que verifique el cumplimiento de los requerimientos del ENS.

Con carácter extraordinario, deberá realizarse dicha auditoría siempre que se produzcan modificaciones sustanciales en los sistemas de información, que puedan repercutir en las medidas de seguridad requeridas. La realización de la auditoria extraordinaria determinará la fecha de cómputo para el cálculo de los dos años, establecidos para la realización de la siguiente auditoría regular ordinaria, indicados en el párrafo anterior.

El plazo de dos años señalado en los párrafos anteriores podrá extenderse durante tres meses cuando concurran impedimentos de fuerza mayor no imputables a la entidad titular del sistema o sistemas de información concernidos.

2. La auditoría se realizará en función de la categoría del sistema y, en su caso, del perfil de cumplimiento específico que corresponda, según lo dispuesto en los anexos I y III y de conformidad con lo regulado en la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.

3. En la realización de las auditorías de la seguridad se utilizarán los criterios, métodos de trabajo y de conducta generalmente reconocidos, así como la normalización nacional e internacional aplicables a este tipo de actividades.

4. El informe de auditoría deberá dictaminar sobre el grado de cumplimiento de este real decreto identificando los hallazgos de cumplimiento e incumplimiento detectados. Deberá, igualmente, incluir los criterios metodológicos de auditoría utilizados, el alcance y el objetivo de la auditoría, y los datos, hechos y observaciones en que se basen las conclusiones formuladas, todo ello de conformidad con la citada Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.

5. Los informes de auditoría serán presentados al responsable del sistema y al responsable de la seguridad. Estos informes serán analizados por este último que presentará sus conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.

6. En el caso de los sistemas de categoría ALTA, visto el dictamen de auditoría y atendiendo a una eventual gravedad de las deficiencias encontradas, el responsable del sistema podrá suspender temporalmente el tratamiento de informaciones, la prestación de servicios o la total operación del sistema, hasta su adecuada subsanación o mitigación.

7. Los informes de auditoría podrán ser requeridos por los responsables de cada organización, con competencias sobre seguridad de las tecnologías de la información, y por el CCN.

Artículo 32. *Informe del estado de la seguridad.*

1. La Comisión Sectorial de Administración Electrónica recogerá la información relacionada con el estado de las principales variables de la seguridad en los sistemas de información a los que se refiere este real decreto, de forma que permita elaborar un perfil general del estado de la seguridad en las entidades titulares de los sistemas de información comprendidos en el ámbito de aplicación del artículo 2, que se plasmará en el informe correspondiente.

2. El CCN articulará los procedimientos necesarios para la recogida y consolidación de la información, así como los aspectos metodológicos para su tratamiento y explotación, a través de los correspondientes grupos de trabajo que se constituyan al efecto en la Comisión Sectorial de Administración Electrónica y en los órganos colegiados competentes en el ámbito de la Administración General del Estado.

3. Los resultados del informe serán utilizados por las autoridades competentes que impulsarán las medidas oportunas que faciliten la mejora continua del estado de la seguridad utilizando en su caso, cuadros de mando e indicadores que contribuyan a la toma de decisiones mediante el uso de las herramientas que el CCN provea para tal efecto.

Artículo 33. *Capacidad de respuesta a incidentes de seguridad.*

1. El CCN articulará la respuesta a los incidentes de seguridad en torno a la estructura denominada CCN-CERT (por su acrónimo en inglés de *Computer Emergency Response Team),* que actuará sin perjuicio de las capacidades de respuesta a incidentes de seguridad que pueda tener cada administración pública y de la función de coordinación a nivel nacional e internacional del CCN.

2. Sin perjuicio de lo establecido en el artículo 19.4 del Real Decreto-ley 12/2018, de 7 de septiembre, las entidades del sector público notificarán al CCN aquellos incidentes que tengan un impacto significativo en la seguridad de los sistemas de información concernidos, de acuerdo con la correspondiente Instrucción Técnica de Seguridad.

3. Cuando un operador esencial que haya sido designado como operador crítico sufra un incidente, los CSIRT de referencia se coordinarán con el Ministerio del Interior, a través de su Oficina de Coordinación de Ciberseguridad, según lo previsto en el artículo 11.2 del Real Decreto-ley 12/2018, de 7 de septiembre.

4. Cuando un operador con incidencia en la Defensa Nacional sufra un incidente deberá analizar si, por su alcance, éste pudiera tener impacto en el funcionamiento del Ministerio de Defensa o en la operatividad de las Fuerzas Armadas, lo pondrá de inmediato en conocimiento de su CSIRT de referencia, quien informará a la capacidad de respuesta e incidentes de seguridad de referencia para el ámbito de la Defensa nacional, denominada ESPDEF-CERT, del Mando Conjunto del Ciberespacio (MCCE) a través de los canales establecidos. En estos casos, el ESPDEF-CERT del Mando Conjunto del Ciberespacio deberá ser oportunamente informado de la evolución de la gestión del incidente y podrá colaborar en la supervisión con la autoridad competente.

5. De conformidad con lo dispuesto en el Real Decreto-ley 12/2018, de 7 de septiembre, el CCN ejercerá la coordinación nacional de la respuesta técnica de los equipos de respuesta a incidentes de seguridad informática (denominados por su acrónimo en inglés *Computer Security Incident Response Team,* en adelante, CSIRT) en materia de seguridad de las redes y sistemas de información del sector público.

6. Tras un incidente de seguridad, el CCN-CERT determinará técnicamente el riesgo de reconexión del sistema o sistemas afectados, indicando los procedimientos a seguir y las salvaguardas a implementar con objeto de reducir el impacto para, en la medida de lo posible, evitar que vuelvan a darse las circunstancias que lo propiciaron.

Tras un incidente de seguridad, la Secretaría General de Administración Digital, sin perjuicio de la normativa que regula la continuidad de los sistemas de información implicados en la seguridad pública o la normativa que regule la continuidad de los sistemas de información militares implicados en la Defensa Nacional que requieran la participación del ESPDEF-CERT del Mando Conjunto del Ciberespacio, autorizará la reconexión a los medios y servicios comunes comprendidos bajo su ámbito de responsabilidad, incluidos los compartidos o transversales, si un informe de superficie de exposición del CCN-CERT hubiere determinado que el riesgo es asumible.

En caso de que se trate de un incidente de seguridad que afecte a un medio o servicio común bajo ámbito de responsabilidad de la Intervención General de la Administración del Estado, esta participará en el proceso de autorización de la reconexión a que se refiere el párrafo anterior.

7. Las organizaciones del sector privado que presten servicios a las entidades públicas notificarán al INCIBE-CERT, centro de respuesta a incidentes de seguridad de referencia para los ciudadanos y entidades de derecho privado en España operado por la S.M.E. Instituto Nacional de Ciberseguridad de España M.P., S.A. (INCIBE) dependiente del Ministerio de Asuntos Económicos y Transformación Digital, los incidentes que les afecten a través de su equipo de respuesta a incidentes de seguridad informática, quien, sin perjuicio de sus competencias y de lo previsto en los artículos 9, 10 y 11 del Real Decreto 43/2021, de

26 de enero, en relación con la Plataforma de Notificación y Seguimiento de Ciberincidentes, lo pondrá inmediatamente en conocimiento del CCN-CERT.

Artículo 34. *Prestación de servicios de respuesta a incidentes de seguridad a las entidades del sector público.*

1. De acuerdo con lo previsto en el artículo 33, el CCN-CERT prestará los siguientes servicios:

a) Soporte y coordinación para el tratamiento de vulnerabilidades y la resolución de incidentes de seguridad que tengan las entidades del ámbito de aplicación de este real decreto.

El CCN-CERT, a través de su servicio de apoyo técnico y de coordinación, actuará con la máxima celeridad ante cualquier agresión recibida en los sistemas de información afectados.

Para el cumplimiento de los fines indicados en los párrafos anteriores se podrán recabar informes, registros de auditoría y configuraciones de los sistemas afectados y cualquier otra información que se considere relevante, así como los soportes informáticos que se estimen necesarios para la investigación del incidente de los sistemas afectados, sin perjuicio de lo dispuesto en la normativa de protección de datos que resulte de aplicación, así como de la posible confidencialidad de datos de carácter institucional u organizativo.

b) Investigación y divulgación de las mejores prácticas sobre seguridad de la información entre todos los miembros de las entidades del sector público. Con esta finalidad, las series de documentos CCN-STIC (CCN-Seguridad de las Tecnologías de Información y la Comunicación), elaboradas por el CCN, ofrecerán normas, instrucciones, guías, recomendaciones y mejores prácticas para aplicar el ENS y para garantizar la seguridad de los sistemas de información del ámbito de aplicación de este real decreto.

c) Formación destinada al personal del sector público especialista en el campo de la seguridad de las tecnologías de la información, al objeto de facilitar la actualización de conocimientos y de lograr la sensibilización y mejora de sus capacidades para la prevención, detección y gestión de incidentes.

d) Información sobre vulnerabilidades, alertas y avisos de nuevas amenazas a los sistemas de información, recopiladas de diversas fuentes de reconocido prestigio, incluidas las propias.

2. El CCN desarrollará un programa que ofrezca la información, formación, recomendaciones y herramientas necesarias para que las entidades del sector público puedan desarrollar sus propias capacidades de respuesta a incidentes de seguridad, y en el que, aquel, será coordinador a nivel público estatal.

CAPÍTULO V

Normas de conformidad

Artículo 35. *Administración digital.*

1. La seguridad de los sistemas de información que sustentan la administración digital se regirá por lo establecido en este real decreto.

2. El CCN es el órgano competente para garantizar la debida interoperabilidad en materia de ciberseguridad y criptografía, en relación con la aplicación del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la administración electrónica.

Artículo 36. *Ciclo de vida de servicios y sistemas.*

Las especificaciones de seguridad se incluirán en el ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.

Artículo 37. *Mecanismos de control.*

Cada entidad titular de los sistemas de información comprendidos en el ámbito de aplicación de este real decreto y, en su caso, sus organismos, órganos, departamentos o

unidades, establecerán sus mecanismos de control para garantizar de forma real y efectiva el cumplimiento del ENS.

Artículo 38. *Procedimientos de determinación de la conformidad con el Esquema Nacional de Seguridad.*

1. Los sistemas de información comprendidos en el ámbito del artículo 2 serán objeto de un proceso para determinar su conformidad con el ENS. A tal efecto, los sistemas de categoría MEDIA o ALTA precisarán de una auditoría para la certificación de su conformidad, sin perjuicio de la auditoría de la seguridad prevista en el artículo 31 que podrá servir asimismo para los fines de la certificación, mientras que los sistemas de categoría BÁSICA solo requerirán de una autoevaluación para su declaración de la conformidad, sin perjuicio de que se puedan someter igualmente a una auditoria de certificación.

Tanto el procedimiento de autoevaluación como la auditoría de certificación se realizarán según lo dispuesto en el artículo 31 y el anexo III y en los términos que se determinen en la correspondiente Instrucción Técnica de Seguridad, que concretará asimismo los requisitos exigibles a las entidades certificadoras.

2. Los sujetos responsables de los sistemas de información a que se refiere el apartado anterior darán publicidad, en los correspondientes portales de internet o sedes electrónicas a las declaraciones y certificaciones de conformidad con el ENS, atendiendo a lo dispuesto en la mencionada Instrucción Técnica de Seguridad.

CAPÍTULO VI

Actualización del Esquema Nacional de Seguridad

Artículo 39. *Actualización permanente.*

El ENS se mantendrá actualizado de manera permanente, desarrollándose y perfeccionándose a lo largo del tiempo, en paralelo al avance de los servicios prestados por las entidades del sector público, la evolución tecnológica, la aparición o consolidación de nuevos estándares internacionales sobre seguridad y auditoría y los riesgos a los que estén expuestos los sistemas de información concernidos.

CAPÍTULO VII

Categorización de los sistemas de información

Artículo 40. *Categorías de seguridad.*

1. La categoría de seguridad de un sistema de información modulará el equilibrio entre la importancia de la información que maneja y los servicios que presta y el esfuerzo de seguridad requerido, en función de los riesgos a los que está expuesto, bajo el principio de proporcionalidad.

2. La determinación de la categoría de seguridad se efectuará en función de la valoración del impacto que tendría un incidente que afectase a la seguridad de la información o de los servicios con perjuicio para la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad, siguiendo el procedimiento descrito en el anexo I.

Artículo 41. *Facultades.*

1. La facultad para efectuar las valoraciones a las que se refiere el artículo 40, así como, en su caso, su posterior modificación, corresponderá al responsable o responsables de la información o servicios afectados.

2. Con base en las valoraciones señaladas en el apartado anterior, la determinación de la categoría de seguridad del sistema corresponderá al responsable o responsables de la seguridad.

Disposición adicional primera. *Formación.*

El CCN y el Instituto Nacional de Administración Pública desarrollarán programas de sensibilización, concienciación y formación, dirigidos al personal de las entidades del sector público, para asegurar un adecuado despliegue de la información y las capacidades jurídicas, organizativas y técnicas relacionadas con la ciberseguridad de los sistemas de información públicos, y para garantizar el conocimiento permanente del ENS entre dichas entidades.

Disposición adicional segunda. *Desarrollo del Esquema Nacional de Seguridad.*

En desarrollo de lo dispuesto en este real decreto, la persona titular del Ministerio para la Transformación Digital y de la Función Pública, a propuesta de la Comisión Sectorial de Administración Electrónica y a iniciativa del Centro Criptológico Nacional, aprobará las instrucciones técnicas de seguridad de obligado cumplimiento, que se publicarán mediante Resolución de la persona titular de la Secretaría de Estado de Función Pública.

Las instrucciones técnicas de seguridad tendrán en cuenta las normas armonizadas por la Unión Europea aplicables. Para su redacción y mantenimiento se constituirán los correspondientes grupos de trabajo en los órganos colegiados con competencias en materia de administración digital.

Para el mejor cumplimiento de lo establecido en este real decreto, el CCN, en el ejercicio de sus competencias, elaborará y difundirá las correspondientes guías de seguridad de las tecnologías de la información y la comunicación (guías CCN-STIC), particularmente de la serie 800, que se incorporarán al conjunto documental utilizado para la realización de las auditorías de seguridad.

Disposición adicional tercera. *Respeto del principio de «no causar un perjuicio significativo» al medioambiente.*

En cumplimiento con lo dispuesto en el Plan de Recuperación, Transformación y Resiliencia (PRTR) y en el Reglamento (UE) 2021/241 del Parlamento Europeo y del Consejo, de 12 de febrero de 2021, por el que se establece el Mecanismo de Recuperación y Resiliencia, todas las actuaciones que se lleven a cabo en el marco del PRTR en cumplimiento del presente real decreto deben respetar el principio de «no causar un perjuicio significativo» al medioambiente (principio DNSH por sus siglas en inglés, *Do No Significant Harm)* y las condiciones del etiquetado climático y digital.

Disposición transitoria única. *Adecuación de sistemas.*

1. Los sistemas de información del ámbito de aplicación de este real decreto, preexistentes a su entrada en vigor, incluidos aquellos de los que sean titulares los contratistas del sector privado en los términos señalados en el artículo 2, dispondrán de veinticuatro meses para alcanzar su plena adecuación al ENS, circunstancia que se manifestará con la exhibición del correspondiente distintivo de conformidad, atendiendo lo dispuesto en el artículo 38.

2. Durante los antedichos veinticuatro meses, los sistemas de información preexistentes a la entrada en vigor de este real decreto que dispusieren de los correspondientes Distintivos de Conformidad, derivados de Declaraciones o Certificaciones de conformidad con el ENS, podrán mantener su vigencia procediendo a su renovación de conformidad y en los términos señalados por el Real Decreto 3/2010, de 8 de enero, del que trajeron causa.

3. Los nuevos sistemas de información aplicarán lo establecido en este real decreto desde su concepción.

Disposición derogatoria única. *Derogación normativa.*

Queda derogado el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, así como cuantas disposiciones de igual o inferior rango que se opongan a lo dispuesto en este real decreto.

Disposición final primera. *Títulos competenciales.*

Este real decreto se dicta en virtud de lo establecido en los artículos 149.1.18.ª, 149.1.21.ª y 149.1.29.ª de la Constitución, que atribuyen al Estado la competencia exclusiva sobre las bases del régimen jurídico de las administraciones públicas, las telecomunicaciones y la seguridad pública, respectivamente.

Disposición final segunda. *Desarrollo normativo.*

Se habilita a la persona titular del Ministerio de Asuntos Económicos y Transformación Digital para dictar las disposiciones necesarias para la aplicación y desarrollo de lo establecido en este real decreto, sin perjuicio de las competencias de las comunidades autónomas de desarrollo y ejecución de la legislación básica del Estado.

Disposición final tercera. *Entrada en vigor.*

Este real decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

ANEXO I

Categorías de seguridad de los sistemas de información

1. Fundamentos para la determinación de la categoría de seguridad de un sistema de información

La determinación de la categoría de seguridad de un sistema de información se basará en la valoración del impacto que tendría sobre la organización un incidente que afectase a la seguridad de la información tratada o de los servicios prestados para:

a) Alcanzar sus objetivos.
b) Proteger los activos a su cargo.
c) Garantizar la conformidad con el ordenamiento jurídico.

Anualmente, o siempre que se produzcan modificaciones significativas en los citados criterios de determinación, deberá re-evaluarse la categoría de seguridad de los sistemas de información concernidos.

2. Dimensiones de la seguridad

A fin de determinar el impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información tratada o de los servicios prestados y, en su consecuencia, establecer la categoría de seguridad del sistema de información en cuestión, se tendrán en cuenta las siguientes dimensiones de la seguridad, que se identificarán por sus correspondientes iniciales en mayúsculas:

a) Confidencialidad [C].
b) Integridad [I].
c) Trazabilidad [T].
d) Autenticidad [A].
e) Disponibilidad [D].

3. Determinación del nivel de seguridad requerido en una dimensión de seguridad

Una información o un servicio pueden verse afectados en una o más de sus dimensiones de seguridad. Cada dimensión de seguridad afectada se adscribirá a uno de los siguientes niveles de seguridad: BAJO, MEDIO o ALTO. Si una dimensión de seguridad no se ve afectada, no se adscribirá a ningún nivel.

a) Nivel BAJO. Se aplicará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio limitado sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

Se entenderá por perjuicio limitado:

1.º La reducción de forma apreciable de la capacidad de la organización para desarrollar eficazmente sus funciones y competencias, aunque estas sigan desempeñándose.
2.º Causar un daño menor en los activos de la organización.
3.º El incumplimiento formal de alguna ley o regulación, que tenga carácter de subsanable.
4.º Causar un perjuicio menor a algún individuo, que pese a resultar molesto, pueda ser fácilmente reparable.
5.º Otros de naturaleza análoga.

b) Nivel MEDIO. Se aplicará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.
Se entenderá por perjuicio grave:

1.º La reducción significativa de la capacidad de la organización para desarrollar eficazmente sus funciones y competencias, aunque estas sigan desempeñándose.
2.º Causar un daño significativo en los activos de la organización.
3.º El incumplimiento material de alguna ley o regulación, o el incumplimiento formal que no tenga carácter de subsanable.
4.º Causar un perjuicio significativo a algún individuo, de difícil reparación.
5.º Otros de naturaleza análoga.

c) Nivel ALTO. Se aplicará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio muy grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.
Se entenderá por perjuicio muy grave:

1.º La anulación efectiva de la capacidad de la organización para desarrollar eficazmente sus funciones y competencias.
2.º Causar un daño muy grave, e incluso irreparable, de los activos de la organización.
3.º El incumplimiento grave de alguna ley o regulación.
4.º Causar un perjuicio grave a algún individuo, de difícil o imposible reparación.
5.º Otros de naturaleza análoga.

Cuando un sistema de información trate diferentes informaciones y preste diferentes servicios, el nivel de seguridad del sistema en cada dimensión será el mayor de los establecidos para cada información y cada servicio.

4. Determinación de la categoría de seguridad de un sistema de información

1. Se definen tres categorías de seguridad: BÁSICA, MEDIA y ALTA.

a) Un sistema de información será de categoría ALTA si alguna de sus dimensiones de seguridad alcanza el nivel de seguridad ALTO.
b) Un sistema de información será de categoría MEDIA si alguna de sus dimensiones de seguridad alcanza el nivel de seguridad MEDIO, y ninguna alcanza un nivel de seguridad superior.
c) Un sistema de información será de categoría BÁSICA si alguna de sus dimensiones de seguridad alcanza el nivel BAJO, y ninguna alcanza un nivel superior.

2. La determinación de la categoría de seguridad de un sistema de información sobre la base de lo indicado en el apartado anterior, no implicará que se altere, por este hecho, el nivel de seguridad de las dimensiones de seguridad que no han influido en la determinación de la categoría de seguridad del mismo.

5. Secuencia de actuaciones para determinar la categoría de seguridad de un sistema

1. Identificación del nivel de seguridad correspondiente a cada información y servicio, en función de las dimensiones de seguridad, teniendo en cuenta lo establecido en el apartado 3 anterior.

2. Determinación de la categoría de seguridad del sistema, según lo establecido en el apartado 4 anterior.

Las guías CCN-STIC, del CCN, precisarán los criterios necesarios para una adecuada categorización de seguridad de los sistemas de información.

ANEXO II

Medidas de Seguridad

1. Disposiciones generales

1. Para lograr el cumplimiento de los principios básicos y requisitos mínimos establecidos se aplicarán las medidas de seguridad indicadas en este anexo, las cuales serán proporcionales a:

a) Las dimensiones de seguridad relevantes en el sistema a proteger.
b) La categoría de seguridad del sistema de información a proteger.

2. Las medidas de seguridad se dividen en tres grupos:

a) Marco organizativo [org]. Constituido por el conjunto de medidas relacionadas con la organización global de la seguridad.
b) Marco operacional [op]. Formado por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin.
c) Medidas de protección [mp]. Se centran en proteger activos concretos, según su naturaleza y la calidad exigida por el nivel de seguridad de las dimensiones afectadas.

2. Selección de medidas de seguridad

1. Para la selección de las medidas de seguridad se seguirán los pasos siguientes:

a) Identificación de los tipos de activos presentes.
b) Determinación de las dimensiones de seguridad relevantes, teniendo en cuenta lo establecido en el anexo I.
c) Determinación del nivel de seguridad correspondiente a cada dimensión de seguridad, teniendo en cuenta lo establecido en el anexo I.
d) Determinación de la categoría de seguridad del sistema, según lo establecido en el anexo I.
e) Selección de las medidas de seguridad, junto con los refuerzos apropiados, de entre las contenidas en este anexo, de acuerdo con las dimensiones y sus niveles de seguridad y para determinadas medidas de seguridad, de acuerdo con la categoría de seguridad del sistema.

2. A los efectos de facilitar el cumplimiento de lo dispuesto en este anexo, cuando en un sistema de información existan subsistemas que requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad con los refuerzos correspondientes, y siempre que puedan delimitarse la información y los servicios afectados.

3. Las guías CCN-STIC, del CCN, podrán establecer perfiles de cumplimiento específicos, según el artículo 30 de este real decreto, para entidades o sectores concretos, que incluirán la relación de medidas y refuerzos que en cada caso resulten aplicables o los criterios para su determinación.

4. La correspondencia entre los niveles de seguridad exigidos en cada dimensión y las medidas de seguridad con sus refuerzos, es la que se indica en la tabla siguiente:

Medidas de Seguridad		Por categoría o dimensión(es)	Nivel de las dimensiones de seguridad		
			BAJO	MEDIO	ALTO
			Categoría de seguridad del sistema		
			BÁSICA	MEDIA	ALTA
org	**Marco organizativo**				
org.1	Política de seguridad	Categoría	aplica	aplica	aplica
org.2	Normativa de seguridad	Categoría	aplica	aplica	aplica

Medidas de Seguridad		Por categoría o dimensión(es)	Nivel de las dimensiones de seguridad		
			BAJO	MEDIO	ALTO
			Categoría de seguridad del sistema		
			BÁSICA	MEDIA	ALTA
org.3	Procedimientos de seguridad	Categoría	aplica	aplica	aplica
org.4	Proceso de autorización	Categoría	aplica	aplica	aplica
op	**Marco operacional**				
op.pl	Planificación				
op.pl.1	Análisis de riesgos	Categoría	aplica	+ R1	+ R2
op.pl.2	Arquitectura de Seguridad	Categoría	aplica	+ R1	+ R1 + R2 + R3
op.pl.3	Adquisición de nuevos componentes	Categoría	aplica	aplica	aplica
op.pl.4	Dimensionamiento/gestión de la capacidad	D	aplica	+ R1	+ R1
op.pl.5	Componentes certificados	Categoría	n.a.	aplica	aplica
op.acc	Control de acceso				
op.acc.1	Identificación	T A	aplica	+ R1	+ R1
op.acc.2	Requisitos de acceso	C I T A	aplica	aplica	+ R1
op.acc.3	Segregación de funciones y tareas	C I T A	n.a.	aplica	+ R1
op.acc.4	Proceso de gestión de derechos de acceso	C I T A	aplica	aplica	aplica
op.acc.5	Mecanismo de autenticación (usuarios externos)	C I T A	+ [R1 o R2 o R3 o R4]	+ [R2 o R3 o R4] + R5	+ [R2 o R3 o R4] + R5
op.acc.6	Mecanismo de autenticación (usuarios de la organización)	C I T A	+ [R1 o R2 o R3 o R4] + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R6 + R7 + R8 + R9
op.exp	Explotación				
op.exp.1	Inventario de activos	Categoría	aplica	aplica	aplica
op.exp.2	Configuración de seguridad	Categoría	aplica	aplica	aplica
op.exp.3	Gestión de la configuración de seguridad	Categoría	aplica	+ R1	+ R1 + R2 + R3
op.exp.4	Mantenimiento y actualizaciones de seguridad	Categoría	aplica	+ R1	+ R1 + R2
op.exp.5	Gestión de cambios	Categoría	n.a.	aplica	+ R1
op.exp.6	Protección frente a código dañino	Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4
op.exp.7	Gestión de incidentes	Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3
op.exp.8	Registro de la actividad	T	aplica	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4 + R5
op.exp.9	Registro de la gestión de incidentes	Categoría	aplica	aplica	aplica
op.exp.10	Protección de claves criptográficas	Categoría	aplica	+ R1	+ R1
op.ext	Recursos externos				
op.ext.1	Contratación y acuerdos de nivel de servicio	Categoría	n.a.	aplica	aplica
op.ext.2	Gestión diaria	Categoría	n.a.	aplica	aplica
op.ext.3	Protección de la cadena de suministro	Categoría	n.a.	n.a.	aplica
op.ext.4	Interconexión de sistemas	Categoría	n.a.	aplica	+ R1
op.nub	Servicios en la nube				
op.nub.1	Protección de servicios en la nube	Categoría	aplica	+ R1	+ R1 + R2
op.cont	Continuidad del servicio				
op.cont.1	Análisis de impacto	D	n.a.	aplica	aplica
op.cont.2	Plan de continuidad	D	n.a.	n.a.	aplica
op.cont.3	Pruebas periódicas	D	n.a.	n.a.	aplica
op.cont.4	Medios alternativos	D	n.a.	n.a.	aplica
op.mon	Monitorización del sistema				
op.mon.1	Detección de intrusión	Categoría	aplica	+ R1	+ R1 + R2
op.mon.2	Sistema de métricas	Categoría	aplica	+ R1 + R2	+ R1 + R2
op.mon.3	Vigilancia	Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4 + R5 + R6
mp	Medidas de protección				
mp.if	Protección de las instalaciones e infraestructuras				
mp.if.1	Áreas separadas y con control de acceso	Categoría	aplica	aplica	aplica
mp.if.2	Identificación de las personas	Categoría	aplica	aplica	aplica
mp.if.3	Acondicionamiento de los locales	Categoría	aplica	aplica	aplica
mp.if.4	Energía eléctrica	D	aplica	+ R1	+ R1
mp.if.5	Protección frente a incendios	D	aplica	aplica	aplica
mp.if.6	Protección frente a inundaciones	D	n.a.	aplica	aplica
mp.if.7	Registro de entrada y salida de equipamiento	Categoría	aplica	aplica	aplica
mp.per	Gestión del personal				
mp.per.1	Caracterización del puesto de trabajo	Categoría	n.a.	aplica	aplica
mp.per.2	Deberes y obligaciones	Categoría	aplica	+ R1	+ R1
mp.per.3	Concienciación	Categoría	aplica	aplica	aplica
mp.per.4	Formación	Categoría	aplica	aplica	aplica
mp.eq	Protección de los equipos				
mp.eq.1	Puesto de trabajo despejado	Categoría	aplica	+ R1	+ R1
mp.eq.2	Bloqueo de puesto de trabajo	A	n.a.	aplica	+ R1
mp.eq.3	Protección de dispositivos portátiles	Categoría	aplica	aplica	+ R1 + R2
mp.eq.4	Otros dispositivos conectados a la red	C	aplica	+ R1	+ R1
mp.com	Protección de las comunicaciones				
mp.com.1	Perímetro seguro	Categoría	aplica	aplica	aplica
mp.com.2	Protección de la confidencialidad	C	aplica	+ R1	+ R1 + R2 + R3
mp.com.3	Protección de la integridad y de la autenticidad	I A	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4
mp.com.4	Separación de flujos de información en la red	Categoría	n.a.	+ [R1 o R2 o R3]	+ [R2 o R3] + R4
mp.si	Protección de los soportes de información				
mp.si.1	Marcado de soportes	C	n.a.	aplica	aplica
mp.si.2	Criptografía	C I	n.a.	aplica	+ R1 + R2
mp.si.3	Custodia	Categoría	aplica	aplica	aplica
mp.si.4	Transporte	Categoría	aplica	aplica	aplica
mp.si.5	Borrado y destrucción	C	aplica	+ R1	+ R1

Medidas de Seguridad		Por categoría o dimensión(es)	Nivel de las dimensiones de seguridad		
			BAJO	MEDIO	ALTO
			Categoría de seguridad del sistema		
			BÁSICA	MEDIA	ALTA
mp.sw	Protección de las aplicaciones informáticas				
mp.sw.1	Desarrollo de aplicaciones	Categoría	n.a.	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4
mp.sw.2	Aceptación y puesta en servicio	Categoría	aplica	+ R1	+ R1
mp.info	Protección de la información				
mp.info.1	Datos personales	Categoría	aplica	aplica	aplica
mp.info.2	Calificación de la información	C	n.a.	aplica	aplica
mp.info.3	Firma electrónica	I A	aplica	+ R1 + R2 + R3	+ R1 + R2 + R3 + R4
mp.info.4	Sellos de tiempo	T	n.a.	n.a.	aplica
mp.info.5	Limpieza de documentos	C	aplica	aplica	aplica
mp.info.6	Copias de seguridad	D	aplica	+ R1	+ R1 + R2
mp.s	Protección de los servicios				
mp.s.1	Protección del correo electrónico	Categoría	aplica	aplica	aplica
mp.s.2	Protección de servicios y aplicaciones web	Categoría	+ [R1 o R2]	+ [R1 o R2]	+ R2 + R3
mp.s.3	Protección de la navegación web	Categoría	aplica	aplica	+ R1
mp.s.4	Protección frente a denegación de servicio	D	n.a.	aplica	+ R1

5. En las tablas del presente anexo se han empleado las siguientes convenciones:

a) La tercera columna indica si la medida se exige atendiendo al nivel de seguridad de una o más dimensiones de seguridad, o atendiendo a la categoría de seguridad del sistema. Cuando se exija por nivel de seguridad de las dimensiones, se indican cuales afectan utilizando sus iniciales.

b) Para indicar que una determinada medida de seguridad se debe aplicar a una o varias dimensiones de seguridad, en algún nivel de seguridad determinado, se utiliza la voz «aplica».

c) «n.a.» significa «no aplica» a efectos de cumplimiento normativo, por lo que no es exigible, sin perjuicio de que su implantación en el sistema pudiera ser beneficioso técnicamente.

d) Para indicar una mayor exigencia se emplean los refuerzos de seguridad (R) que se suman (+) a los requisitos base de la medida pero que no siempre son incrementales entre sí.

e) Para señalar que se puede elegir entre aplicar un refuerzo u otro, se indicará entre corchetes y separados por «o» [Rn o Rn+1].

f) Se han empleado los colores verde, amarillo y rojo con el siguiente código: verde para indicar que una medida se aplica en sistemas de categoría BÁSICA o superior; el amarillo para indicar qué medidas y refuerzos empiezan a aplicar en categoría MEDIA o superior; y el rojo para indicar qué medidas o refuerzos son solo de aplicación en categoría ALTA o requieren un esfuerzo en seguridad superior al de categoría MEDIA.

6. A continuación, se describen individualmente cada una de las medidas organizadas de la siguiente forma:

a) Primero, una tabla resumen con las exigencias de seguridad de la medida en función de la categoría de seguridad del sistema y de las dimensiones de seguridad afectadas.

b) A continuación, una descripción con el cuerpo de la medida que desglosa los requisitos de base.

c) Posteriormente, podrán aparecer una serie de refuerzos adicionales que complementan a los requisitos de base, no en todos los casos requeridos o exigidos, y que podrían aplicarse en determinados perfiles de cumplimiento específicos.

d) Además, se indica el conjunto de requisitos y refuerzos exigidos en función de los niveles de seguridad o de la categoría de seguridad del sistema, según corresponda. En los casos en los que se pueda elegir entre aplicar un refuerzo u otro, además de indicarlo entre corchetes [Rm o Rn], se incluirá un diagrama de flujo explicativo.

e) Por último, algunos refuerzos son de carácter opcional, no siendo requeridos en todos los sistemas de información. Se aplicarán como medidas adicionales cuando el análisis de riesgos así lo recomiende.

3. Marco organizativo [ORG]

El marco organizativo está constituido por un conjunto de medidas relacionadas con la organización global de la seguridad.

3.1 Política de seguridad [org.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

La política de seguridad, que se aprobará de conformidad con lo dispuesto en el artículo 12 de este real decreto, se plasmará en un documento en el que, de forma clara, se precise, al menos, lo siguiente:

– [org.1.1] Los objetivos o misión de la organización.
– [org.1.2] El marco legal y regulatorio en el que se desarrollarán las actividades.
– [org.1.3] Los roles o funciones de seguridad, definiendo para cada uno los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación.
– [org.1.4] La estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, las personas integrantes y la relación con otros elementos de la organización.
– [org.1.5] Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

Aplicación de la medida.

– Categoría BÁSICA: org.1.
– Categoría MEDIA: org.1.
– Categoría ALTA: org.1.

3.2 Normativa de seguridad [org.2].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

Se dispondrá de una serie de documentos que describan:

– [org.2.1] El uso correcto de equipos, servicios e instalaciones, así como lo que se considerará uso indebido.
– [org.2.2] La responsabilidad del personal con respecto al cumplimiento o violación de la normativa: derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente.

Refuerzo R1-Documentos específicos.

[org.2.r1.1] Se dispondrá de una documentación de seguridad, desarrollada según lo reflejado en las guías CCN-STIC que resulten de aplicación.

Aplicación de la medida.

– Categoría BÁSICA: org.2.
– Categoría MEDIA: org.2.
– Categoría ALTA: org.2.

3.3 Procedimientos de seguridad [org.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA

	aplica	aplica	aplica

Requisitos.

Se dispondrá de una serie de documentos que detallen de forma clara y precisa cómo operar los elementos del sistema de información:

– [org.3.1] Cómo llevar a cabo las tareas habituales.
– [org.3.2] Quién debe hacer cada tarea.
– [org.3.3] Cómo identificar y reportar comportamientos anómalos.
– [org.3.4.] La forma en que se ha de tratar la información en consideración al nivel de seguridad que requiere, precisando cómo efectuar:

a) Su control de acceso.
b) Su almacenamiento.
c) La realización de copias.
d) El etiquetado de soportes.
e) Su transmisión telemática.
f) Cualquier otra actividad relacionada con dicha información.

Refuerzo R1-Validación de procedimientos.

[org.3.r1.1] Se requerirá la validación de los procedimientos de seguridad por la autoridad correspondiente.

Aplicación de la medida.

– Categoría BÁSICA: org.3.
– Categoría MEDIA: org.3.
– Categoría ALTA: org.3.

3.4 Proceso de autorización [org.4].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

Se establecerá un proceso formal de autorizaciones que cubra todos los elementos del sistema de información concernidos:

– [org.4.1] Utilización de instalaciones, habituales y alternativas.
– [org.4.2] Entrada de equipos en producción, en particular, equipos que involucren criptografía.
– [org.4.3] Entrada de aplicaciones en producción.
– [org.4.4] Establecimiento de enlaces de comunicaciones con otros sistemas.
– [org.4.5] Utilización de medios de comunicación, habituales y alternativos.
– [org.4.6] Utilización de soportes de información.
– [org.4.7] Utilización de equipos móviles. Se entenderá por equipos móviles ordenadores portátiles, tabletas, teléfonos móviles u otros de naturaleza análoga.
– [org.4.8] Utilización de servicios de terceros, bajo contrato o convenio, concesión, encargo, etc.

Aplicación de la medida.

– Categoría BÁSICA: org.4.
– Categoría MEDIA: org.4.
– Categoría ALTA: org.4.

4. Marco operacional [op]

El marco operacional está constituido por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin.

4.1 Planificación [op.pl].

4.1.1 Análisis de riesgos [op.pl.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+ R2

Requisitos.

Se realizará un análisis de riesgos informal, realizado en lenguaje natural. Es decir, una exposición textual que:

– [op.pl.1.1] Identifique los activos más valiosos del sistema. (Ver op.exp.1).
– [op.pl.1.2] Identifique las amenazas más probables.
– [op.pl.1.3] Identifique las salvaguardas que protegen de dichas amenazas.
– [op.pl.1.4] Identifique los principales riesgos residuales.

Refuerzo R1-Análisis de riesgos semiformal.

Se deberá realizar un análisis de riesgos semiformal, usando un lenguaje específico, con un catálogo básico de amenazas y una semántica definida. Es decir, una presentación con tablas que:

– [op.pl.1.r1.1] Valore cualitativamente los activos más valiosos del sistema.
– [op.pl.1.r1.2] Cuantifique las amenazas más probables.
– [op.pl.1.r1.3] Valore las salvaguardas que protegen de dichas amenazas.
– [op.pl.1.r1.4] Valore el riesgo residual.

Refuerzo R2-Análisis de riesgos formal.

Se deberá realizar un análisis formal, usando un lenguaje específico, con un fundamento matemático reconocido internacionalmente, que:

– [op.pl.1.r2.1] Valore cualitativamente los activos más valiosos del sistema.
– [op.pl.1.r2.2] Cuantifique las amenazas posibles.
– [op.pl.1.r2.3] Valore y priorice las salvaguardas adecuadas.
– [op.pl.1.r2.4] Valore y asuma formalmente el riesgo residual.

Aplicación de la medida.

– Categoría BÁSICA: op.pl.1.
– Categoría MEDIA: op.pl.1 + R1.
– Categoría ALTA: op.pl.1 + R2.

4.1.2 Arquitectura de seguridad [op.pl.2].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+R1+R2+R3

Requisitos.

La seguridad del sistema será objeto de un planteamiento integral detallando, al menos, los siguientes aspectos:

– [op.pl.2.1] Documentación de las instalaciones, incluyendo áreas y puntos de acceso.
– [op.pl.2.2] Documentación del sistema, incluyendo equipos, redes internas y conexiones al exterior, y puntos de acceso al sistema (puestos de trabajo y consolas de administración).
– [op.pl.2.3] Esquema de líneas de defensa, incluyendo puntos de interconexión a otros sistemas o a otras redes (en especial, si se trata de internet o redes públicas en general); cortafuegos, DMZ, etc.; y la utilización de tecnologías diferentes para prevenir vulnerabilidades que pudieran perforar simultáneamente varias líneas de defensa.

– [op.pl.2.4] Sistema de identificación y autenticación de usuarios, incluyendo el uso de claves concertadas, contraseñas, tarjetas de identificación, biometría, u otras de naturaleza análoga, y el uso de ficheros o directorios para autenticar al usuario y determinar sus derechos de acceso.

Refuerzo R1-Sistema de gestión.

[op.pl.2.r1.1] Sistema de gestión, relativo a la planificación, organización y control de los recursos relativos a la seguridad de la información.

Refuerzo R2-Sistema de gestión de la seguridad con mejora continua.

[op.pl.2.r2.1] Sistema de gestión de la seguridad de la información, con actualización y aprobación periódica.

Refuerzo R3-Validación de datos.

[op.pl.2.r3.1] Controles técnicos internos, incluyendo la validación de datos de entrada, salida y datos intermedios.

Aplicación de la medida.

– Categoría BÁSICA: op.pl.2.
– Categoría MEDIA: op.pl.2 + R1.
– Categoría ALTA: op.pl.2 + R1 + R2 + R3.

4.1.3 Adquisición de nuevos componentes [op.pl.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

Se establecerá un proceso formal para planificar la adquisición de nuevos componentes del sistema, proceso que:

– [op.pl.3.1] Atenderá a las conclusiones del análisis de riesgos ([op.pl.1]).
– [op.pl.3.2] Será acorde a la arquitectura de seguridad escogida ([op.pl.2]).
– [op.pl.3.3] Contemplará las necesidades técnicas, de formación y de financiación, de forma conjunta.

Aplicación de la medida.

– Categoría BÁSICA: op.pl.3.
– Categoría MEDIA: op.pl.3.
– Categoría ALTA: op.pl.3.

4.1.4 Dimensionamiento / gestión de la capacidad [op.pl.4].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	aplica	+ R1	+ R1

Requisitos.

Con carácter previo a la puesta en explotación, se realizará un estudio que cubrirá los siguientes aspectos:

– [op.pl.4.1] Necesidades de procesamiento.
– [op.pl.4.2] Necesidades de almacenamiento de información: durante su procesamiento y durante el periodo que deba retenerse.
– [op.pl.4.3] Necesidades de comunicación.
– [op.pl.4.4] Necesidades de personal: cantidad y cualificación profesional.
– [op.pl.4.5] Necesidades de instalaciones y medios auxiliares.

Refuerzo R1 –Mejora continua de la gestión de la capacidad.

– [op.pl.4.r1.1] Se realizará una previsión de la capacidad y se mantendrá actualizada durante todo el ciclo de vida del sistema.
– [op.pl.4.r1.2] Se emplearán herramientas y recursos para la monitorización de la capacidad.

Aplicación de la medida (por disponibilidad):

– Nivel BAJO: op.pl.4.
– Nivel MEDIO: op.pl.4 + R1.
– Nivel ALTO: op.pl.4 + R1.

4.1.5 Componentes certificados [op.pl.5].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	aplica	aplica

Requisitos.

– [op.pl.5.1]. Se utilizará el Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y Comunicación (CPSTIC) del CCN, para seleccionar los productos o servicios suministrados por un tercero que formen parte de la arquitectura de seguridad del sistema y aquellos que se referencien expresamente en las medidas de este real decreto.
En caso de que no existan productos o servicios en el CPSTIC que implementen las funcionalidades requeridas, se utilizarán productos certificados de acuerdo a lo descrito en el artículo 19.
Una Instrucción Técnica de Seguridad detallará los criterios relativos a la adquisición de productos de seguridad.
– [op.pl.5.2] Si el sistema suministra un servicio de seguridad a un tercero bajo el alcance del ENS, el producto o productos que en los que se sustente dicho servicio debe superar un proceso de cualificación y ser incluido en el CPSTIC, o aportar una certificación que cumpla con los requisitos funcionales de seguridad y de aseguramiento de acuerdo a lo establecido en el artículo 19.

Refuerzo R1-Protección de emisiones electromagnéticas.

[op.pl.5.r1.1] La información deberá ser protegida frente a las amenazas TEMPEST de acuerdo con la normativa en vigor.

Refuerzo R2 - Lista de componentes software.

[op.pl.5.r2.1] Cada producto y servicio incluirá en su descripción una lista de componentes software, acorde a lo especificado en [mp.sw.1.r5].

Aplicación de la medida.

– Categoría BÁSICA: no aplica.
– Categoría MEDIA: op.pl.5.
– Categoría ALTA: op.pl.5.

4.2 Control de acceso [op.acc].

El control de acceso comprende el conjunto de actividades preparatorias y ejecutivas tendentes a permitir o denegar a una entidad, usuario o proceso, el acceso a un recurso del sistema para la realización de una acción concreta.
Los mecanismos de control de acceso deberán equilibrar la facilidad de uso y la protección de la información y los servicios, primando una u otra característica atendiendo a la categoría de seguridad del sistema.
Cuando se interconecten sistemas en los que la identificación, autenticación y autorización tengan lugar en diferentes dominios de seguridad, bajo distintas responsabilidades, en los casos en que sea necesario, las medidas de seguridad locales se

acompañarán de los correspondientes acuerdos de colaboración que delimiten mecanismos y procedimientos para la atribución y ejercicio efectivos de las responsabilidades de cada sistema ([op.ext]).

4.2.1 Identificación [op.acc.1].

dimensiones	T A		
nivel	BAJO	MEDIO	ALTO
	aplica	+ R1	+ R1

Requisitos.

La identificación de los usuarios del sistema se realizará de acuerdo con lo que se indica a continuación:

– [op.acc.1.1] Se podrá utilizar como identificador único los sistemas de identificación previstos en la normativa de aplicación, entre ellos, los sistemas de clave concertada y cualquier otro sistema que las administraciones consideren válido en los términos y condiciones establecidos en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

– [op.acc.1.2] Cuando el usuario tenga diferentes roles frente al sistema (como ciudadano o usuario final, como trabajador del organismo o como administrador de los sistemas, por ejemplo) recibirá identificadores singulares para cada perfil, de forma que se recaben siempre los correspondientes registros de actividad, delimitándose los privilegios correspondientes a cada perfil.

– [op.acc.1.3] Cada entidad (entidad, usuario o proceso) que accede al sistema, contará con un identificador singular que permita conocer el destinatario de los mismos y los derechos de acceso que recibe, así como las acciones realizadas por cada entidad.

– [op.acc.1.4] Las cuentas de usuario se gestionarán de la siguiente forma:

a) Cada cuenta (de entidad, usuario o proceso) estará asociada a un identificador único.

b) Las cuentas deben ser inhabilitadas en los siguientes casos: cuando el usuario deja la organización; cuando el usuario cesa en la función para la cual se requería la cuenta de usuario; o, cuando la persona que la autorizó da orden en sentido contrario.

c) Las cuentas se retendrán durante el periodo necesario para atender a las necesidades de trazabilidad de los registros de actividad asociados a las mismas. A este periodo se le denominará «periodo de retención».

– [op.acc.1.5] En los supuestos de comunicaciones electrónicas, las partes intervinientes se identificarán atendiendo a los mecanismos previstos en la legislación europea y nacional en la materia, con la siguiente correspondencia entre los niveles de la dimensión de autenticidad de los sistemas de información a los que se tiene acceso y los niveles de seguridad (bajo, sustancial, alto) de los sistemas de identificación electrónica previstos en el Reglamento (UE) n.º 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE y sus normas de desarrollo o ejecución que resulten de aplicación:

a) Si se requiere un nivel BAJO en la dimensión de autenticidad (anexo I): Nivel de seguridad bajo, sustancial o alto (artículo 8 del Reglamento (UE) n.º 910/2014).

b) Si se requiere un nivel MEDIO en la dimensión de autenticidad (anexo I): Nivel de seguridad sustancial o alto (artículo 8 del Reglamento (UE) n.º 910/2014).

c) Si se requiere un nivel ALTO en la dimensión de autenticidad (anexo I): Nivel de seguridad alto (artículo 8 del Reglamento (UE) n.º 910/2014).

Refuerzo R1-Identificación avanzada.

– [op.acc.1.r1.1] La identificación del usuario permitirá al Responsable del Sistema, al Responsable de la Seguridad o a sus respectivos administradores delegados, singularizar a la persona asociada al mismo, así como sus responsabilidades en el sistema.

– [op.acc.1.r1.2] Los datos de identificación serán utilizados por el sistema para determinar los privilegios del usuario conforme a los requisitos de control de acceso establecidos en la documentación de seguridad.
– [op.acc.1.r1.3] Se asegurará la existencia de una lista actualizada de usuarios autorizados y mantenida por el administrador del sistema/de la seguridad del sistema.

Aplicación de la medida (por trazabilidad y autenticidad).

– Nivel BAJO: op.acc.1.
– Nivel MEDIO: op.acc.1 +R1.
– Nivel ALTO: op.acc.1+ R1.

4.2.2 Requisitos de acceso [op.acc.2].

dimensiones	C I T A		
nivel	BAJO	MEDIO	ALTO
	aplica	aplica	+ R1

Requisitos.

– [op.acc.2.1] Los recursos del sistema se protegerán con algún mecanismo que impida su utilización, salvo a las entidades que disfruten de derechos de acceso suficientes.
– [op.acc.2.2] Los derechos de acceso de cada recurso, se establecerán según las decisiones de la persona responsable del recurso, ateniéndose a la política y normativa de seguridad del sistema.
– [op.acc.2.3] Particularmente, se controlará el acceso a los componentes del sistema operativo y a sus ficheros o registros de configuración.

Refuerzo R1-Privilegios de acceso.

– [op.acc.2.r1.1] Todos los usuarios autorizados deben tener un conjunto de atributos de seguridad (privilegios) que puedan ser mantenidos individualmente.
– [op.acc.2.r1.2] Los privilegios de acceso se implementarán para restringir el tipo de acceso que un usuario puede tener (lectura, escritura, modificación, borrado, etc.).

Refuerzo R2-Control de acceso a dispositivos.

– [op.acc.2.r2.1] Se dispondrá de soluciones que permitan establecer controles de acceso a los dispositivos en función de la política de seguridad de la organización.

Aplicación de la medida (por confidencialidad, integridad, trazabilidad y autenticidad).

– Nivel BAJO: op.acc.2.
– Nivel MEDIO: op.acc.2.
– Nivel ALTO: op.acc.2+ R1.

4.2.3 Segregación de funciones y tareas [op.acc.3].

dimensiones	C I T A		
nivel	BAJO	MEDIO	ALTO
	n.a.	aplica	+ R1

Requisitos.

El sistema de control de acceso se organizará de forma que se exija la concurrencia de dos o más personas para realizar tareas críticas, anulando la posibilidad de que un solo individuo autorizado pueda abusar de sus derechos para cometer alguna acción ilícita o no autorizada.

– [op.acc.3.1] Siempre que sea posible, las capacidades de desarrollo y operación no recaerán en la misma persona.
– [op.acc.3.2] Siempre que sea posible, las personas que autorizan y controlan el uso serán distintas.

Refuerzo R1-Segregación rigurosa.

– [op.acc.3.r1.1] Siempre que sea posible, la misma persona no aunará funciones de configuración y mantenimiento del sistema.
– [op.acc.3.r1.2] La misma persona no puede aunar funciones de auditoría o supervisión con cualquier otra función.

Refuerzo R2-Privilegios de auditoría.

– [op.acc.3.r2.1] Existirán cuentas con privilegios de auditoría estrictamente controladas y personalizadas.

Refuerzo R3-Acceso a la información de seguridad.

– [op.acc.3.r3.1] El acceso a la información de seguridad del sistema estará permitido únicamente a los administradores de seguridad/sistema autorizados, utilizando los mecanismos de acceso imprescindibles (consola, interfaz web, acceso remoto, etc.).

Aplicación de la medida (por confidencialidad, integridad, trazabilidad y autenticidad).

– Nivel BAJO: no aplica.
– Nivel MEDIO: op.acc.3.
– Nivel ALTO: op.acc.3 + R1.

4.2.4 Proceso de gestión de derechos de acceso [op.acc.4].

dimensiones	C I T A		
nivel	BAJO	MEDIO	ALTO
	aplica	aplica	aplica

Requisitos.

Los derechos de acceso de cada entidad, usuario o proceso se limitarán atendiendo a los siguientes principios:

– [op.acc.4.1] Todo acceso estará prohibido, salvo autorización expresa.
– [op.acc.4.2] Mínimo privilegio: los privilegios de cada entidad, usuario o proceso se reducirán al mínimo imprescindible para cumplir sus obligaciones o funciones.
– [op.acc.4.3] Necesidad de conocer y responsabilidad de compartir: los privilegios se asignarán de forma que las entidades, usuarios o procesos sólo accederán al conocimiento de aquella información requerida para cumplir sus obligaciones o funciones. La información es patrimonio del organismo y toda aquella que resulte necesaria para el usuario estará a su disposición.
– [op.acc.4.4] Capacidad de autorizar: Exclusivamente el personal con competencia para ello podrá conceder, alterar o anular la autorización de acceso a los recursos, conforme a los criterios establecidos por su responsable. Los permisos de acceso se revisarán de forma periódica.
– [op.acc.4.5] Se establecerá una política específica de acceso remoto, requiriéndose autorización expresa.

Aplicación de la medida (por confidencialidad, integridad, trazabilidad y autenticidad).

Nivel BAJO: op.acc.4.
Nivel MEDIO: op.acc.4.
Nivel ALTO: op.acc.4.

4.2.5 Mecanismo de autenticación (usuarios externos) [op.acc.5].

Referente a usuarios que no son usuarios de la organización.
Las guías CCN-STIC desarrollarán los mecanismos y calidades exigibles a cada tipo de factor de autenticación en función de los niveles de seguridad requeridos por el sistema de información el que se accede y los privilegios concedidos al usuario.

dimensiones	C I T A

nivel	BAJO	MEDIO	ALTO
	+ [R1 o R2 o R3 o R4]	+ [R2 o R3 o R4] + R5	+ [R2 o R3 o R4] + R5

Requisitos.

– [op.acc.5.1] Antes de proporcionar las credenciales de autenticación a las entidades, usuarios o procesos, estos deberán haberse identificado y registrado de manera fidedigna ante el sistema o ante un Prestador Cualificado de Servicios de Confianza o un proveedor de identidad electrónica reconocido por las administraciones públicas, de conformidad con lo dispuesto en la Ley 39/2015, de 1 de octubre.

– [op.acc.5.2] Antes de activar el mecanismo de autenticación, el usuario reconocerá que las ha recibido y que conoce y acepta las obligaciones que implica su tenencia, en particular, el deber de custodia diligente, la protección de su confidencialidad y el deber de notificación inmediata en caso de pérdida.

– [op.acc.5.3] Las credenciales estarán bajo el control exclusivo del usuario y se activarán una vez estén bajo su control efectivo.

– [op.acc.5.4] Las credenciales se cambiarán con una periodicidad marcada por la política de seguridad de la organización.

– [op.acc.5.5] Las credenciales serán inhabilitadas -pudiendo ser regeneradas, en su caso-, cuando conste o se sospeche su pérdida, compromiso o revelación a entidades (personas, equipos o procesos) no autorizadas.

– [op.acc.5.6] Las credenciales serán inhabilitadas cuando la entidad (persona, equipo o proceso) que autentican termina su relación con el sistema.

– [op.acc.5.7] Antes de autorizar el acceso, la información presentada por el sistema será la mínima imprescindible para que el usuario se autentique, evitando todo aquello que pueda, directa o indirectamente, revelar información sobre el sistema o la cuenta, sus características, su operación o su estado. Las credenciales solamente se validarán cuando se tengan todos los datos necesarios y, si se rechaza, no se informará del motivo del rechazo.

– [op.acc.5.8] El número de intentos permitidos será limitado, bloqueando la oportunidad de acceso una vez superado tal número, y requiriendo una intervención específica para reactivar la cuenta, que se describirá en la documentación.

– [op.acc.5.9] El sistema informará al usuario de sus derechos u obligaciones inmediatamente después de obtener el acceso.

Refuerzo R1-Contraseñas.

– [op.acc.5.r1.1] Se empleará una contraseña como mecanismo de autenticación.

– [op.acc.5.r1.2] Se impondrán normas de complejidad mínima y robustez frente a ataques de adivinación (ver guías CCN-STIC).

Refuerzo R2-Contraseña + OTP.

– [op.acc.5.r2.1] Se requerirá una contraseña de un solo uso (OTP, en inglés) como complemento a la contraseña de usuario.

Refuerzo R3-Certificados.

– [op.acc.5.r3.1] Se emplearán certificados cualificados como mecanismo de autenticación.

– [op.acc.5.r3.2] El uso del certificado estará protegido por un segundo factor, del tipo PIN o biométrico.

– [op.acc.5.r3.3] Las credenciales utilizadas deberán haber sido obtenidas tras un registro previo presencial, o bien telemático, usando un certificado electrónico cualificado.

Refuerzo R4-Certificados en dispositivo físico.

– [op.acc.5.r4.1] Se emplearán certificados cualificados como mecanismo de autenticación, en soporte físico (tarjeta o similar) usando algoritmos, parámetros y dispositivos autorizados por el CCN.

– [op.acc.5.r4.2] El uso del certificado estará protegido por un segundo factor, del tipo PIN o biométrico.

– [op.acc.5.r4.3] Las credenciales utilizadas deberán haber sido obtenidas tras un registro previo presencial, o bien telemático, usando certificado electrónico cualificado.

Refuerzo R5-Registro.

– [op.acc.5.r5.1] Se registrarán los accesos con éxito y los fallidos.
– [op.acc.5.r5.2] Se informará al usuario del último acceso efectuado con su identidad.

Refuerzo R6-Limitación de la ventana de acceso.

– [op.acc.5.r6.1] Se definirán aquellos puntos en los que el sistema requerirá una renovación de la autenticación del usuario, mediante identificación singular, no bastando con la sesión establecida.

Refuerzo R7-Suspensión por no utilización.

– [op.acc.5.r7.1] Las credenciales se suspenderán tras un periodo definido de no utilización.

Aplicación de la medida (por confidencialidad, integridad, trazabilidad y autenticidad).

– Nivel BAJO: op.acc.5 + [R1 o R2 o R3 o R4].
– Nivel MEDIO: op.acc.5 + [R2 o R3 o R4] + R5.
– Nivel ALTO: op.acc.5 + [R2 o R3 o R4] + R5.

4.2.6 Mecanismo de autenticación (usuarios de la organización) [op.acc.6].

Esta medida se refiere a personal del organismo, propio o contratado, estable o circunstancial, que pueda tener acceso a información contenida en el sistema.

Las guías CCN-STIC desarrollarán los mecanismos y calidades exigibles a cada tipo de factor de autenticación, en función de los niveles de seguridad requeridos por el sistema de información el que se accede y los privilegios concedidos al usuario.

dimensiones	C I T A		
nivel	BAJO	MEDIO	ALTO
	+ [R1 o R2 o R3 o R4] + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R6 + R7 + R8 + R9

Requisitos.

– [op.acc.6.1] Antes de proporcionar las credenciales a los usuarios, estos deberán conocer y aceptar la política de seguridad del organismo en los aspectos que les afecten.

– [op.acc.6.2] Antes de activar el mecanismo de autenticación, el usuario reconocerá que ha recibido las credenciales de acceso y que conoce y acepta las obligaciones que implica su tenencia, en particular, el deber de custodia diligente, la protección de su confidencialidad y el deber de notificación inmediata en caso de pérdida.

– [op.acc.6.3] Las credenciales estarán bajo el control exclusivo del usuario y se activarán una vez estén bajo su control efectivo.

– [op.acc.6.4] Las credenciales se cambiarán con una periodicidad marcada por la política de seguridad de la organización.

– [op.acc.6.5] Las credenciales serán inhabilitadas -pudiendo ser regeneradas, en su caso-, cuando conste o se sospeche su pérdida, compromiso o revelación a entidades (personas, equipos o procesos) no autorizadas.

– [op.acc.6.6] Las credenciales serán inhabilitadas cuando el usuario que autentican termina su relación con el sistema.

– [op.acc.6.7] Antes de autorizar el acceso, la información presentada por el sistema será la mínima imprescindible para que el usuario se autentique, evitando todo aquello que pueda, directa o indirectamente, revelar información sobre el sistema o la cuenta, sus características, su operación o su estado. Las credenciales solamente se validarán cuando se tengan todos los datos necesarios y, si se rechaza, no se informará del motivo del rechazo.

– [op.acc.6.8] El número de intentos permitidos será limitado, bloqueando la oportunidad de acceso una vez superado tal número, y requiriendo una intervención específica para reactivar la cuenta, que se describirá en la documentación.
– [op.acc.6.9] El sistema informará al usuario de sus derechos u obligaciones inmediatamente después de obtener el acceso.

Refuerzo R1-Contraseñas.

– [op.acc.6.r1.1] Se empleará una contraseña como mecanismo de autenticación cuando el acceso se realiza desde zonas controladas y sin atravesar zonas no controladas (véase refuerzo R8).
– [op.acc.6.r1.2] Se impondrán normas de complejidad mínima y robustez frente a ataques de adivinación (ver guías CCN-STIC).

Refuerzo R2-Contraseña + otro factor de autenticación.

– [op.acc.6.r2.1] Se requerirá un segundo factor tal como «algo que se tiene», es decir, un dispositivo, una contraseña de un solo uso (OTP, en inglés) como complemento a la contraseña de usuario, o «algo que se es».

Refuerzo R3-Certificados.

– [op.acc.6.r3.1] Se emplearán certificados cualificados como mecanismo de autenticación.
– [op.acc.6.r3.2] El uso del certificado estará protegido por un segundo factor, del tipo PIN o biométrico.

Refuerzo R4-Certificados en dispositivo físico.

– [op.acc.6.r4.1] Se emplearán certificados cualificados como mecanismo de autenticación, en soporte físico (tarjeta o similar) usando algoritmos, parámetros y dispositivos autorizados por el CCN.
– [op.acc.6.r4.2] El uso del certificado estará protegido por un segundo factor, del tipo PIN o biométrico.

Refuerzo R5-Registro.

– [op.acc.6.r5.1] Se registrarán los accesos con éxito y los fallidos.
– [op.acc.6.r5.2] Se informará al usuario del último acceso efectuado con su identidad.

Refuerzo R6-Limitación de la ventana de acceso.

– [op.acc.6.r6.1] Se definirán aquellos puntos en los que el sistema requerirá una renovación de la autenticación del usuario, mediante identificación singular, no bastando con la sesión establecida.

Refuerzo R7-Suspensión por no utilización.

– [op.acc.6.r7.1] Las credenciales se suspenderán tras un periodo definido de no utilización.

Refuerzo R8-Doble factor para acceso desde o a través de zonas no controladas.

Se denomina «zona controlada» aquella que no es de acceso público, requiriéndose que el usuario, antes de tener acceso al equipo, se haya autenticado previamente de alguna forma (control de acceso a las instalaciones), diferente del mecanismo de autenticación lógica frente al sistema. Un ejemplo de zona no controlada es Internet.

– [op.acc.6.r8.1] Para el acceso desde o a través de zonas no controladas se requerirá un doble factor de autenticación: R2, R3 o R4.

Refuerzo R9-Acceso remoto (todos los niveles).

– [op.acc.6.r9.1] Será de aplicación la ITS de Interconexión de sistemas de información.
– [op.acc.6.r9.2] El acceso remoto deberá considerar los siguientes aspectos:

a) Ser autorizado por la autoridad correspondiente.
b) El tráfico deberá ser cifrado.

c) Si la utilización no se produce de manera constante, el acceso remoto deberá encontrarse inhabilitado y habilitarse únicamente cuando sea necesario.
d) Deberán recogerse registros de auditoría de este tipo de conexiones.

Aplicación de la medida (por confidencialidad, integridad, trazabilidad y autenticidad).

– Nivel BAJO: op.acc.6 + [R1 o R2 o R3 o R4] + R8 + R9.
– Nivel MEDIO: op.acc.6 + [R1 o R2 o R3 o R4] + R5 + R8 + R9.
– Nivel ALTO: op.acc.6 + [R1 o R2 o R3 o R4] + R5 + R6 + R7 + R8 + R9.

4.3 Explotación [op.exp].

4.3.1 Inventario de activos [op.exp.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

[op.exp.1.1] Se mantendrá un inventario actualizado de todos los elementos del sistema, detallando su naturaleza e identificando a su responsable; es decir, la persona que toma las decisiones relativas al mismo.

Refuerzo R1-Inventario de etiquetado.

– [op.exp.1.r1.1] El etiquetado del equipamiento y del cableado formará parte del inventario.

Refuerzo R2-Identificación periódica de activos.

– [op.exp.1.r2.1] Se dispondrá de herramientas que permitan visualizar de forma continua el estado de todos los equipos en la red, en particular, los servidores y los dispositivos de red y de comunicaciones.

Refuerzo R3-Identificación de activos críticos.

– [op.exp.1.r3.1] Se dispondrá de herramientas que permitan categorizar los activos críticos por contexto de la organización y riesgos de seguridad.

Refuerzo R4-Lista de componentes software.

– [op.exp.1.r4.1] Se mantendrá actualizada una relación formal de los componentes software de terceros empleados en el despliegue del sistema. Esta lista incluirá librerías software y los servicios requeridos para su despliegue (plataforma o entorno operacional). El contenido de la lista de componentes será equivalente a lo requerido en [mp.sw.1.r5].

Aplicación de la medida.

– Categoría BÁSICA: op.exp.1.
– Categoría MEDIA: op.exp.1.
– Categoría ALTA: op.exp.1.

4.3.2 Configuración de seguridad [op.exp.2].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

Se configurarán los equipos previamente a su entrada en operación, de forma que:

– [op.exp.2.1] Se retiren cuentas y contraseñas estándar.
– [op.exp.2.2] Se aplicará la regla de «mínima funcionalidad», es decir:

a) El sistema debe proporcionar la funcionalidad mínima imprescindible para que la organización alcance sus objetivos.
b) No proporcionará funciones injustificadas (de operación, administración o auditoría) al objeto de reducir al mínimo su perímetro de exposición, eliminándose o desactivándose aquellas funciones que sean innecesarias o inadecuadas al fin que se persigue.

– [op.exp.2.3] Se aplicará la regla de «seguridad por defecto», es decir:

a) Las medidas de seguridad serán respetuosas con el usuario y protegerán a éste, salvo que se exponga conscientemente a un riesgo.
b) Para reducir la seguridad, el usuario tendrá que realizar acciones conscientes.
c) El uso natural, en los casos que el usuario no ha consultado el manual, será un uso seguro.

– [op.exp.2.4] Las máquinas virtuales estarán configuradas y gestionadas de un modo seguro. La gestión del parcheado, cuentas de usuarios, software antivirus, etc. se realizará como si se tratara de máquinas físicas, incluyendo la máquina anfitriona.

Aplicación de la medida.

– Categoría BÁSICA: op.exp.2.
– Categoría MEDIA: op.exp.2.
– Categoría ALTA: op.exp.2.

4.3.3 Gestión de la configuración de seguridad [op.exp.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+R1+R2+R3

Requisitos.

Se gestionará de forma continua la configuración de los componentes del sistema, de forma que:

– [op.exp.3.1] Se mantenga en todo momento la regla de "funcionalidad mínima" ([op.exp.2]).
– [op.exp.3.2] Se mantenga en todo momento la regla de "mínimo privilegio" ([op.exp.2]).
– [op.exp.3.3] El sistema se adapte a las nuevas necesidades, previamente autorizadas. (Ver [op.acc.4]).
– [op.exp.3.4] El sistema reaccione a vulnerabilidades notificadas. (Ver [op.exp.4]).
– [op.exp.3.5] El sistema reaccione a incidentes. (Ver [op.exp.7]).
– [op.exp.3.6] La configuración de seguridad solamente podrá editarse por personal debidamente autorizado.

Refuerzo R1-Mantenimiento regular de la configuración.

– [op.exp.3.r1.1] Existirán configuraciones hardware/software, autorizadas y mantenidas regularmente, para los servidores, elementos de red y estaciones de trabajo.
– [op.exp.3.r1.2] Se verificará periódicamente la configuración hardware/software del sistema para asegurar que no se han introducido ni instalado elementos no autorizados.
– [op.exp.3.r1.3] Se mantendrá una lista de servicios autorizados para servidores y estaciones de trabajo.

Refuerzo R2-Responsabilidad de la configuración.
– [op.exp.3.r2.1] La configuración de seguridad del sistema operativo y aplicaciones, tanto de estaciones y servidores como de la electrónica de red del sistema, será responsabilidad de un número muy limitado de administradores del sistema.

Refuerzo R3-Copias de seguridad.

– [op.exp.3.r3.1] Se realizarán copias de seguridad de la configuración del sistema de forma que sea posible reconstruirlo en parte o en su totalidad tras un incidente.

Refuerzo R4-Aplicación de la configuración.

– [op.exp.3.r4.1] La configuración de seguridad del sistema operativo y de las aplicaciones se mantendrá actualizada a través de una aplicación o procedimiento manual que permita la instalación de las correspondientes modificaciones de versión y actualizaciones de seguridad oportunas.

Refuerzo R5-Control del estado de seguridad de la Configuración.

– [op.exp.3.r5.1] Se dispondrá de herramientas que permitan conocer de forma periódica el estado de seguridad de la configuración de los dispositivos de red y, en el caso de que resulte deficiente, permitir su corrección.

Aplicación de la medida.

– Categoría BÁSICA: op.exp.3.
– Categoría MEDIA: op.exp.3 + R1.
– Categoría ALTA: op.exp.3 + R1 + R2 + R3.

4.3.4 Mantenimiento y actualizaciones de seguridad [op.exp.4].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+R1+R2

Requisitos.

Para mantener el equipamiento físico y lógico que constituye el sistema, se aplicará lo siguiente:

– [op.exp.4.1] Se atenderá a las especificaciones de los fabricantes en lo relativo a instalación y mantenimiento de los sistemas, lo que incluirá un seguimiento continuo de los anuncios de defectos.

– [op.exp.4.2] Se dispondrá de un procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones. La priorización tendrá en cuenta la variación del riesgo en función de la implantación o no de la actualización.

– [op.exp.4.3] El mantenimiento solo podrá realizarse por personal debidamente autorizado.

Refuerzo R1-Pruebas en preproducción.

[op.exp.4.r1.1] Antes de poner en producción una nueva versión o una versión parcheada, se comprobará en un entorno de prueba controlado y consistente en configuración al entorno de producción, que la nueva instalación funciona correctamente y no disminuye la eficacia de las funciones necesarias para el trabajo diario.

Refuerzo R2-Prevención de fallos.

[op.exp.4.r2.1] Antes de la aplicación de las configuraciones, parches y actualizaciones de seguridad se preverá un mecanismo para revertirlos en caso de aparición de efectos adversos.

Refuerzo R3-Actualizaciones y pruebas periódicas.

[op.exp.4.r3.1] Se deberá comprobar de forma periódica la integridad del firmware utilizado en los dispositivos hardware del sistema (infraestructura de red, BIOS, etc.). La periodicidad de estas comprobaciones seguirá las recomendaciones de la Guía CCN-STIC que sea de aplicación.

Refuerzo R4 - Monitorización continua.

[op.exp.4.r4.1] Se desplegará a nivel de sistema una estrategia de monitorización continua de amenazas y vulnerabilidades. Esta estrategia detallará:

1. Los indicadores críticos de seguridad a emplear.

2. La política de aplicación de parches de seguridad de los componentes software relacionados en las listas de [op.exp.1.r4], [op.ext.3.r3] y [mp.sw.1.r5]).
3. Los criterios de revisión regular y excepcional de las amenazas sobre el sistema.

Aplicación de la medida.

– Categoría BÁSICA: op.exp.4.
– Categoría MEDIA: op.exp.4 + R1.
– Categoría ALTA: op.exp.4 + R1 + R2.

4.3.5 Gestión de cambios [op.exp.5].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	aplica	+ R1

Requisitos.

Se mantendrá un control continuo de los cambios realizados en el sistema, de forma que:

– [op.exp.5.1] Los cambios se planificarán para reducir el impacto sobre la prestación de los servicios afectados. Para ello, todas las peticiones de cambio se registrarán asignando un número de referencia que permita su seguimiento, de forma equivalente al registro de los incidentes.
– [op.exp.5.2] La información a registrar para cada petición de cambio será suficiente para que quien deba autorizarlos no tenga dudas al respecto y permita gestionarlo hasta su desestimación o implementación.
– [op.exp.5.3] Las pruebas de preproducción, siempre que sea posible realizarlas, se efectuarán en equipos equivalentes a los de producción, al menos en los aspectos específicos del cambio.
– [op.exp.5.4] Mediante un análisis de riesgos se determinará si los cambios son relevantes para la seguridad del sistema. Aquellos cambios que impliquen un riesgo de nivel ALTO deberán ser aprobados, explícitamente, de forma previa a su implantación, por el Responsable de la Seguridad.
– [op.exp.5.5] Una vez implementado el cambio, se realizarán las pruebas de aceptación convenientes. Si son positivas, se actualizará la documentación de configuración (diagramas de red, manuales, el inventario, etc.), siempre que proceda.

Refuerzo R1-Prevención de fallos.

– [op.exp.5.r1.1] Antes de la aplicación de los cambios, se deberá tener en cuenta la posibilidad de revertirlos en caso de la aparición de efectos adversos.
– [op.exp.5.r1.2] Todos los fallos en el software y hardware deberán ser comunicados al responsable designado en la organización de la seguridad.
– [op.exp.5.r1.3] Todos los cambios en el sistema deberán documentarse, incluyendo una valoración del impacto que dicho cambio supone en la seguridad del sistema.

Aplicación de la medida.

– Categoría BÁSICA: no aplica.
– Categoría MEDIA: op.exp.5.
– Categoría ALTA: op.exp.5+ R1.

4.3.6 Protección frente a código dañino [op.exp.6].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1+R2	+R1+R2+R3+R4

Requisitos.

– [op.exp.6.1] Se dispondrá de mecanismos de prevención y reacción frente a código dañino, incluyendo el correspondiente mantenimiento de acuerdo a las recomendaciones del fabricante.

– [op.exp.6.2] Se instalará software de protección frente a código dañino en todos los equipos: puestos de usuario, servidores y elementos perimetrales.

– [op.exp.6.3] Todo fichero procedente de fuentes externas será analizado antes de trabajar con él.

– [op.exp.6.4] Las bases de datos de detección de código dañino permanecerán permanentemente actualizadas.

– [op.exp.6.5] El software de detección de código dañino instalado en los puestos de usuario deberá estar configurado de forma adecuada e implementará protección en tiempo real de acuerdo a las recomendaciones del fabricante.

Refuerzo R1-Escaneo periódico.

– [op.exp.6.r1.1] Todo el sistema se escaneará regularmente para detectar código dañino.

Refuerzo R2-Revisión preventiva del sistema.

– [op.exp.6.r2.1] Las funciones críticas se analizarán al arrancar el sistema en prevención de modificaciones no autorizadas.

Refuerzo R3 - Lista blanca.

– [op.exp.6.r3.1] Solamente se podrán ejecutar aquellas aplicaciones previamente autorizadas. Se implementará una lista blanca para impedir la ejecución de aplicaciones no autorizadas.

Refuerzo R4-Capacidad de respuesta en caso de incidente.

– [op.exp.6.r4.1] Se emplearán herramientas de seguridad orientadas a detectar, investigar y resolver actividades sospechosas en puestos de usuario y servidores (EDR - *Endpoint Detection and Response*).

Refuerzo R5-Configuración de la herramienta de detección de código dañino.

– [op.exp.6.r5.1] El software de detección de código dañino permitirá realizar configuraciones avanzadas y revisar el sistema en el arranque y cada vez que se conecte un dispositivo extraíble.

– [op.exp.6.r5.2] El software de detección de código dañino instalado en servidores y elementos perimetrales deberá estar configurado de forma adecuada e implementará protección en tiempo real de acuerdo a las recomendaciones del fabricante.

Aplicación de la medida.

– Categoría BÁSICA: op.exp.6.
– Categoría MEDIA: op.exp.6+ R1 + R2.
– Categoría ALTA: op.exp.6+ R1 + R2 + R3 + R4.

4.3.7 Gestión de incidentes [op.exp.7].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1+R2	+ R1+R2+ R3

Requisitos.

– [op.exp.7.1] Se dispondrá de un proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema, que incluya el informe de eventos de seguridad y debilidades, detallando los criterios de clasificación y el escalado de la notificación.

– [op.exp.7.2] La gestión de incidentes que afecten a datos personales tendrá en cuenta lo dispuesto en el Reglamento General de Protección de Datos; la Ley Orgánica 3/2018, de 5

de diciembre, en especial su disposición adicional primera, así como el resto de normativa de aplicación, sin perjuicio de los requisitos establecidos en este real decreto.

Refuerzo R1-Notificación.

– [op.exp.7.r1.1] Se dispondrá de soluciones de ventanilla única para la notificación de incidentes al CCN-CERT, que permita la distribución de notificaciones a las diferentes entidades de manera federada, utilizando para ello dependencias administrativas jerárquicas.

Refuerzo R2 –Detección y Respuesta.

El proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema ([op.exp.7.1]) deberá incluir:

– [op.exp.7.r2.1] Implantación de medidas urgentes, incluyendo la detención de servicios, el aislamiento del sistema afectado, la recogida de evidencias y protección de los registros, según convenga al caso.
– [op.exp.7.r2.2] Asignación de recursos para investigar las causas, analizar las consecuencias y resolver el incidente.
– [op.exp.7.r2.3] Informar del incidente a los responsables de la información y servicios afectados y de las actuaciones llevadas a cabo para su resolución.
– [op.exp.7.r2.4] Medidas para:

a) Prevenir que se repita el incidente.
b) Incluir en los procedimientos de usuario la identificación y forma de tratar el incidente.
c) Actualizar, extender, mejorar u optimizar los procedimientos de resolución de incidentes.

Refuerzo R3-Reconfiguración dinámica.

La reconfiguración dinámica del sistema persigue detener, desviar o limitar ataques, acotando los daños.
– [op.exp.7.r3.1] La reconfiguración dinámica incluye, por ejemplo, cambios en las reglas de los enrutadores (*routers*), listas de control de acceso, parámetros del sistema de detección / prevención de intrusiones y reglas en los cortafuegos y puertas de enlace, aislamiento de elementos críticos y aislamiento de las copias de seguridad.
– [op.exp.7.r3.2] El organismo adaptará los procedimientos de reconfiguración dinámica reaccionando a los anuncios recibidos del CCN-CERT relativos a ciberamenazas sofisticadas y campañas de ataques.

Refuerzo R4-Prevención y Respuesta Automática.

– [op.exp.7.r4.1] Se dispondrá de herramientas que automaticen el proceso de prevención y respuesta mediante la detección e identificación de anomalías, la segmentación dinámica de la red para reducir la superficie de ataque, el aislamiento de dispositivos críticos, etc.

Aplicación de la medida.

– Categoría BÁSICA: op.exp.7.
– Categoría MEDIA: op.exp.7+ R1 + R2.
– Categoría ALTA: op.exp.7+ R1 + R2 + R3.

4.3.8 Registro de la actividad [op.exp.8].

dimensiones	T		
nivel	BAJO	MEDIO	ALTO
	aplica	+R1+R2+R3+R4	+R1+R2+R3+R4+R5

Requisitos.

Se registrarán las actividades en el sistema, de forma que:

– [op.exp.8.1] Se generará un registro de auditoría, que incluirá, al menos, el identificador del usuario o entidad asociado al evento, fecha y hora, sobre qué información se realiza el evento, tipo de evento y el resultado del evento (fallo o éxito), según la política de seguridad y los procedimientos asociados a la misma.
– [op.exp.8.2] Se activarán los registros de actividad en los servidores.

Refuerzo R1-Revisión de los registros.

– [op.exp.8.r1.1] Se revisarán informalmente, de forma periódica, los registros de actividad, buscando patrones anormales.

Refuerzo R2-Sincronización del reloj del sistema.

– [op.exp.8.r2.1] El sistema deberá disponer de una referencia de tiempo (*timestamp*) para facilitar las funciones de registro de eventos y auditoría. La modificación de la referencia de tiempo del sistema será una función de administración y, en caso de realizarse su sincronización con otros dispositivos, deberán utilizarse mecanismos de autenticación e integridad.

Refuerzo R3-Retención de registros.

– [op.exp.8.r3.1] En la documentación de seguridad del sistema se deberán indicar los eventos de seguridad que serán auditados y el tiempo de retención de los registros antes de ser eliminados.

Refuerzo R4-Control de acceso.

– [op.exp.8.r4.1] Los registros de actividad y, en su caso, las copias de seguridad de los mismos, solamente podrán ser accedidos o eliminarse por personal debidamente autorizado.

Refuerzo R5-Revisión automática y correlación de eventos.

– [op.exp.8.r5.1] El sistema deberá implementar herramientas para analizar y revisar la actividad del sistema y la información de auditoría, en búsqueda de comprometimientos de la seguridad posibles o reales.
– [op.exp.8.r5.2] Se dispondrá de un sistema automático de recolección de registros, correlación de eventos y respuesta automática ante los mismos.

Aplicación de la medida (por trazabilidad).

– Nivel BAJO: op.exp.8.
– Nivel MEDIO: op.exp.8 + R1 + R2 + R3 + R4.
– Nivel ALTO: op.exp.8 + R1 + R2 + R3 + R4 + R5.

4.3.9 Registro de la gestión de incidentes [op.exp.9].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

Se registrarán todas las actuaciones relacionadas con la gestión de incidentes, de forma que:

– [op.exp.9.1] Se registrarán los reportes iniciales, intermedios y finales de los incidentes, las actuaciones de emergencia y las modificaciones del sistema derivadas del incidente.
– [op.exp.9.2] Se registrará aquella evidencia que pueda dirimirse en un ámbito jurisdiccional, especialmente cuando el incidente pueda comportar acciones disciplinarias sobre el personal interno, sobre proveedores externos o en la persecución de delitos. En la determinación de la composición y detalle de estas evidencias, se recurrirá a asesoramiento legal especializado.
– [op.exp.9.3] Como consecuencia del análisis de los incidentes, se revisará la determinación de los eventos auditables.

Aplicación de la medida.

– Categoría BÁSICA: op.exp.9.
– Categoría MEDIA: op.exp.9.
– Categoría ALTA: op.exp.9.

4.3.10 Protección de claves criptográficas [op.exp.10].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+ R1

Requisitos.

– [op.exp.10.1] Las claves criptográficas se protegerán durante todo su ciclo de vida: (1) generación, (2) transporte al punto de explotación, (3) custodia durante la explotación, (4) archivo posterior a su retirada de explotación activa y (5) destrucción final.
– [op.exp.10.2] Los medios de generación estarán aislados de los medios de explotación.
– [op.exp.10.3] Las claves retiradas de operación que deban ser archivadas, lo serán en medios aislados de los de explotación.

Refuerzo R1-Algoritmos autorizados.

– [op.exp.10.r1.1] Se emplearán algoritmos y parámetros autorizados por el CCN.

Refuerzo R2-Protección avanzada de claves criptográficas.

– [op.exp.10.r2.1] Se emplearán cifradores que cumplan con los requisitos establecidos en la guía CCN-STIC que sea de aplicación.

Aplicación de la medida.

– Categoría BÁSICA: op.exp.10.
– Categoría MEDIA: op.exp.10 + R1.
– Categoría ALTA: op.exp.10 + R1.

4.4 Recursos externos [op.ext].

Cuando la organización utilice recursos externos (servicios, productos, instalaciones o personal), mantendrá la plena responsabilidad de los riesgos para la información tratada o los servicios prestados, debiendo adoptar las medidas necesarias para ejercer su responsabilidad y mantener el control en todo momento.

4.4.1 Contratación y acuerdos de nivel de servicio [op.ext.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	aplica	aplica

Requisitos.

– [op.ext.1.1] Con anterioridad a la efectiva utilización de los recursos externos se establecerá contractualmente un Acuerdo de Nivel de Servicio, que incluirá las características del servicio prestado, lo que debe entenderse como «servicio mínimo admisible», así como, la responsabilidad del prestador y las consecuencias de eventuales incumplimientos.

Aplicación de la medida.

– Categoría BÁSICA: no aplica.
– Categoría MEDIA: op.ext.1.
– Categoría ALTA: op.ext.1.

4.4.2 Gestión diaria [op.ext.2].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	aplica	aplica

Requisitos.

Se establecerá lo siguiente:

– [op.ext.2.1] Un sistema rutinario para medir el cumplimiento de las obligaciones de servicio, incluyendo el procedimiento para neutralizar cualquier desviación fuera del margen de tolerancia acordado ([op.ext.1]).
– [op.ext.2.2] El mecanismo y los procedimientos de coordinación para llevar a cabo las tareas de mantenimiento de los sistemas comprendidos en el acuerdo, que contemplarán los supuestos de incidentes y desastres (ver [op.exp.7]).

Aplicación de la medida.

– Categoría BÁSICA: no aplica.
– Categoría MEDIA: op.ext.2.
– Categoría ALTA: op.ext.2.

4.4.3 Protección de la cadena de suministro [op.ext.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	n.a.	aplica

Requisitos.

– [op.ext.3.1] Se analizará el impacto que puede tener sobre el sistema un incidente accidental o deliberado que tenga su origen en la cadena de suministro.
– [op.ext.3.2] Se estimará el riesgo sobre el sistema por causa del impacto estimado en el punto anterior.
– [op.ext.3.3] Se tomarán medidas de contención de los impactos estimados en los puntos anteriores.

Refuerzo R1-Plan de contingencia.

– [op.ext.3.r1.1] El plan de continuidad de la organización deberá tener en cuenta la dependencia de proveedores externos críticos.
– [op.ext.3.r1.2] Se deberán realizar pruebas o ejercicios de continuidad, incluyendo escenarios en los que falla un proveedor.

Refuerzo R2-Sistema de gestión de la seguridad.

– [op.ext.3.r2.1] Se implementará un sistema de protección de los procesos y flujos de información en las relaciones en línea (*online*) entre los distintos integrantes de la cadena de suministro.

Refuerzo R3-Lista de componentes software.

– [op.ext.3.r3.1] Se mantendrá actualizado un registro formal que contenga los detalles y las relaciones de la cadena de suministro de los diversos componentes utilizados en la construcción de programas informáticos, acorde a lo especificado en [mp.sw.1.r5]. Esta lista será proporcionada por el proveedor de la aplicación, librería o producto suministrado.

Aplicación de la medida.

– Categoría BÁSICA: no aplica.
– Categoría MEDIA: no aplica.
– Categoría ALTA: op.ext.3.

4.4.4 Interconexión de sistemas [op.ext.4].

Se denomina interconexión al establecimiento de enlaces con otros sistemas de información para el intercambio de información y servicios.

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	aplica	+ R1

Requisitos.

– [op.ext.4.1] Todos los intercambios de información y prestación de servicios con otros sistemas deberán ser objeto de una autorización previa. Todo flujo de información estará prohibido salvo autorización expresa.
– [op.ext.4.2] Para cada interconexión se documentará explícitamente: las características de la interfaz, los requisitos de seguridad y protección de datos y la naturaleza de la información intercambiada.

Refuerzo R1-Coordinación de actividades.

– [op.ext.4.r1.1] Cuando se interconecten sistemas en los que la identificación, autenticación y autorización tengan lugar en diferentes dominios de seguridad, bajo distintas responsabilidades, las medidas de seguridad locales se acompañarán de los correspondientes mecanismos y procedimientos de coordinación para la atribución y ejercicio efectivos de las responsabilidades de cada sistema.

Aplicación de la medida.

– Categoría BÁSICA: no aplica.
– Categoría MEDIA: op.ext.4.
– Categoría ALTA: op.ext.4 + R1.

4.5 Servicios en la nube [op.nub].

4.5.1 Protección de servicios en la nube [op.nub.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+R1+R2

Requisitos.

– [op.nub.1.1] Los sistemas que suministran un servicio en la nube a organismos del sector público deberán cumplir con el conjunto de medidas de seguridad en función del modelo de servicio en la nube que presten: Software como Servicio (*Software as a Service, SaaS*), Plataforma como Servicio (*Platform as a Service, PaaS*) e Infraestructura como Servicio (*Infrastructure as a Service, IaaS*) definidas en las guías CCN-STIC que sean de aplicación.
– [op.nub.1.2] Cuando se utilicen servicios en la nube suministrados por terceros, los sistemas de información que los soportan deberán ser conformes con el ENS o cumplir con las medidas desarrolladas en una guía CCN-STIC que incluirá, entre otros, requisitos relativos a:

a) Auditoría de pruebas de penetración (*pentesting*).
b) Transparencia.
c) Cifrado y gestión de claves.
d) Jurisdicción de los datos.

Refuerzo R1- Servicios certificados.

– [op.nub.1.r1.1] Cuando se utilicen servicios en la nube suministrados por terceros, estos deberán estar certificados bajo una metodología de certificación reconocida por el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información.
– [op.nub.1.r1.2] Si el servicio en la nube es un servicio de seguridad deberá cumplir con los requisitos establecidos en [op.pl.5].

Refuerzo R2-Guías de Configuración de Seguridad Específicas.

– [op.nub.1.r2.1] La configuración de seguridad de los sistemas que proporcionan estos servicios deberá realizarse según la correspondiente guía CCN-STIC de Configuración de Seguridad Específica, orientadas tanto al usuario como al proveedor.

Aplicación de la medida.

– Categoría BÁSICA: op.nub.1.
– Categoría MEDIA: op.nub.1 + R1.
– Categoría ALTA: op.nub.1+ R1 + R2.

4.6 Continuidad del servicio [op.cont].

4.6.1 Análisis de impacto [op.cont.1].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	n.a.	aplica	aplica

Requisitos.

– [op.cont.1.1] Se realizará un análisis de impacto que permita determinar los requisitos de disponibilidad de cada servicio (impacto de una interrupción durante un periodo de tiempo determinado), así como los elementos que son críticos para la prestación de cada servicio.

Aplicación de la medida (por disponibilidad).

– Nivel BAJO: no aplica.
– Nivel MEDIO: op.cont.1.
– Nivel ALTO: op.cont.1.

4.6.2 Plan de continuidad [op.cont.2].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	n.a.	n.a.	aplica

Requisitos.

Se desarrollará un plan de continuidad que establezca las acciones a ejecutar en caso de interrupción de los servicios prestados con los medios habituales. Dicho plan contemplará los siguientes aspectos:

– [op.cont.2.1] Se identificarán funciones, responsabilidades y actividades a realizar.
– [op.cont.2.2] Existirá una previsión para coordinar la entrada en servicio de los medios alternativos de forma que se garantice poder seguir prestando los servicios esenciales de la organización.
– [op.cont.2.3] Todos los medios alternativos estarán planificados y materializados en acuerdos o contratos con los proveedores correspondientes.
– [op.cont.2.4] Las personas afectadas por el plan recibirán formación específica relativa a su papel en dicho plan.
– [op.cont.2.5] El plan de continuidad será parte integral y armónica de los planes de continuidad de la organización en otras materias ajenas a la seguridad.

Refuerzo R1-Plan de emergencia y contingencia.

– [op.cont.2.r1.1] Cuando se determine la necesidad de continuidad de los sistemas, deberá existir un plan de emergencia y contingencia en consonancia. En función del análisis de Impacto, se determinarán los aspectos a cubrir.

Refuerzo R2-Comprobación de integridad.

– [op.cont.2.r2.1] Ante una caída o discontinuidad del sistema, se deberá comprobar la integridad del sistema operativo, del firmware y de los ficheros de configuración.

Aplicación de la medida (por disponibilidad).

– Nivel BAJO: no aplica.
– Nivel MEDIO: no aplica.
– Nivel ALTO: op.cont.2.

4.6.3 Pruebas periódicas [op.cont.3].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	n.a.	n.a.	aplica

Requisitos.

– [op.cont.3.1] Se realizarán pruebas periódicas para localizar y, en su caso, corregir los errores o deficiencias que puedan existir en el plan de continuidad.

Aplicación de la medida (por disponibilidad).

– Nivel BAJO: no aplica.
– Nivel MEDIO: no aplica.
– Nivel ALTO: op.cont.3.

4.6.4 Medios alternativos [op.cont.4].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	n.a.	n.a.	aplica

Requisitos.

– [op.cont.4.1] Estará prevista la disponibilidad de medios alternativos para poder seguir prestando servicio cuando los medios habituales no estén disponibles. En concreto, se cubrirán los siguientes elementos del sistema:

a) Servicios contratados a terceros.
b) Instalaciones alternativas.
c) Personal alternativo.
d) Equipamiento informático alternativo.
e) Medios de comunicación alternativos.

– [op.cont.4.2] Se establecerá un tiempo máximo para que los medios alternativos entren en funcionamiento.
– [op.cont.4.3] Los medios alternativos estarán sometidos a las mismas garantías de seguridad que los originales.

Refuerzo R1-Automatización de la transición a medios alternativos.

– [op.cont.4.r1.1] El sistema dispondrá de elementos hardware o software que permitan la transferencia de los servicios automáticamente a los medios alternativos.

Aplicación de la medida (por disponibilidad).

– Nivel BAJO: no aplica.
– Nivel MEDIO: no aplica.
– Nivel ALTO: op.cont.4.

4.7 Monitorización del sistema [op.mon].

El sistema estará sujeto a medidas de monitorización de su actividad y ejecutará acciones predeterminadas en función de las situaciones de compromiso de la seguridad que figuren en el análisis de riesgos. Esto puede incluir la generación de alarmas en tiempo real, la finalización del proceso que está ocasionando la alarma, la inhabilitación de determinados servicios, la desconexión de usuarios y el bloqueo de cuentas.

4.7.1 Detección de intrusión [op.mon.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+R1+R2

Requisitos.

– [op.mon.1.1] Se dispondrá de herramientas de detección o prevención de intrusiones.

Refuerzo R1-Detección basada en reglas.

– [op.mon.1.r1.1] El sistema dispondrá de herramientas de detección o prevención de intrusiones basadas en reglas.

Refuerzo R2-Procedimientos de respuesta.

– [op.mon.1.r2.1] Existirán procedimientos de respuesta a las alertas generadas por el sistema de detección o prevención de intrusiones.

Refuerzo R3-Acciones predeterminadas.

– [op.mon.1.r3.1] El sistema ejecutará automáticamente acciones predeterminadas de respuesta a las alertas generadas. Esto puede incluir la finalización del proceso que está ocasionando la alerta, la inhabilitación de determinados servicios, la desconexión de usuarios y el bloqueo de cuentas.

Aplicación de la medida.

– Categoría BÁSICA: op.mon.1.
– Categoría MEDIA: op.mon.1 + R1.
– Categoría ALTA: op.mon.1+ R1 + R2.

4.7.2 Sistema de métricas [op.mon.2].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1+R2	+ R1+R2

Requisitos.

– [op.mon.2.1] Atendiendo a la categoría de seguridad del sistema, se recopilarán los datos necesarios para conocer el grado de implantación de las medidas de seguridad que resulten aplicables y, en su caso, para proveer el informe anual requerido por el artículo 32.

Refuerzo R1-Efectividad del sistema de gestión de incidentes.

– [op.mon.2.r1.1] Se recopilarán los datos precisos que posibiliten evaluar el comportamiento del sistema de gestión de incidentes, de acuerdo con la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad y con la correspondiente guía CCN-STIC.

Refuerzo R2-Eficiencia del sistema de gestión de la seguridad.

– [op.mon.2.r2.1] Se recopilarán los datos precisos para conocer la eficiencia del sistema de seguridad, en relación con los recursos consumidos, en términos de horas y presupuesto.

Aplicación de la medida.

– Categoría BÁSICA: op.mon.2.
– Categoría MEDIA: op.mon.2 + R1+ R2.
– Categoría ALTA: op.mon.2 + R1 + R2.

4.7.3 Vigilancia [op.mon.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA

	aplica	+ R1+R2	+ R1+R2+R3+R4+R5+R6

Requisitos.

– [op.mon.3.1] Se dispondrá de un sistema automático de recolección de eventos de seguridad.

Refuerzo R1-Correlación de eventos.

– [op.mon.3.r1.1] Se dispondrá de un sistema automático de recolección de eventos de seguridad que permita la correlación de los mismos.

Refuerzo R2-Análisis dinámico.

– [op.mon.3.r2.1] Se dispondrá de soluciones de vigilancia que permitan determinar la superficie de exposición con relación a vulnerabilidades y deficiencias de configuración.

Refuerzo R3-Ciberamenazas avanzadas.

– [op.mon.3.r3.1] Se dispondrá de sistemas para detección de amenazas avanzadas y comportamientos anómalos.
– [op.mon.3.r3.2] Se dispondrá de sistemas para la detección de amenazas persistentes avanzadas (*Advanced Persistent Threat, APT*) mediante la detección de anomalías significativas en el tráfico de la red.

Refuerzo R4-Observatorios digitales.

– [op.mon.3.r4.1] Se dispondrá de observatorios digitales con fines de cibervigilancia dedicados a la detección y seguimiento de anomalías que pudieran representar indicadores de amenaza en contenidos digitales.

Refuerzo R5-Minería de datos.

Se aplicarán medidas para prevenir, detectar y reaccionar frente a intentos de minería de datos:

– [op.mon.3.r5.1] Limitación de las consultas, monitorizando volumen y frecuencia.
– [op.mon.3.r5.2] Alerta a los administradores de seguridad de comportamientos sospechosos en tiempo real.

Refuerzo R6-Inspecciones de seguridad.

Periódicamente, o tras incidentes que hayan desvelado vulnerabilidades del sistema nuevas o subestimadas, se realizarán las siguientes inspecciones:

– [op.mon.3.r6.1] Verificación de configuración.
– [op.mon.3.r6.2] Análisis de vulnerabilidades.
– [op.mon.3.r6.3] Pruebas de penetración.

Refuerzo R7-Interconexiones.

– [op.mon.3.r7.1] En las interconexiones que lo requieran se aplicarán controles en los flujos de intercambio de información a través del uso de metadatos.

Aplicación de la medida.

– Categoría BÁSICA: op.mon.3.
– Categoría MEDIA: op.mon.3 + R1 + R2.
– Categoría ALTA: op.mon.3 + R1 + R2 + R3 + R4 + R5 + R6.

5. Medidas de protección [mp]

Las medidas de protección estarán dirigidas a proteger activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad.

5.1 Protección de las instalaciones e infraestructuras [mp.if].

5.1.1 Áreas separadas y con control de acceso [mp.if.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

– [mp.if.1.1] El equipamiento del Centro de Proceso de Datos (CPD) se instalará, en la medida de lo posible, en áreas separadas, específicas para su función.
– [mp.if.1.2] Se controlarán los accesos a las áreas indicadas de forma que sólo se pueda acceder por las entradas previstas.

Aplicación de la medida.

– Categoría BÁSICA: mp.if.1.
– Categoría MEDIA: mp.if.1.
– Categoría ALTA: mp.if.1.

5.1.2 Identificación de las personas [mp.if.2].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

[mp.if.2.1] El procedimiento de control de acceso identificará a las personas que accedan a los locales donde hay equipamiento esencial que forme parte del sistema de información del CPD, registrando las correspondientes entradas y salidas.

Aplicación de la medida.

– Categoría BÁSICA: mp.if.2.
– Categoría MEDIA: mp.if.2.
– Categoría ALTA: mp.if.2.

5.1.3 Acondicionamiento de los locales [mp.if.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

Los locales donde se ubiquen los sistemas de información y sus componentes esenciales dispondrán de elementos adecuados para el eficaz funcionamiento del equipamiento allí instalado, y, en especial, para asegurar:

– [mp.if.3.1] Las condiciones de temperatura y humedad.
– [mp.if.3.2] La protección frente a las amenazas identificadas en el análisis de riesgos.
– [mp.if.3.3] La protección del cableado frente a incidentes fortuitos o deliberados.

Aplicación de la medida.

– Categoría BÁSICA: mp.if.3.
– Categoría MEDIA: mp.if.3.
– Categoría ALTA: mp.if.3.

5.1.4 Energía eléctrica [mp.if.4].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	aplica	+ R1	+ R1

Requisitos.

– [mp.if.4.1] Los locales donde se ubiquen los sistemas de información y sus componentes esenciales dispondrán de tomas de energía eléctrica, de modo que se garantice el suministro y el correcto funcionamiento de las luces de emergencia.

Refuerzo R1-Suministro eléctrico de emergencia.

– [mp.if.4.r1.1] En caso de fallo del suministro principal, el abastecimiento eléctrico deberá estar garantizado durante el tiempo suficiente para una terminación ordenada de los procesos y la salvaguarda de la información.

Aplicación de la medida (por disponibilidad).

– Nivel BAJO: mp.if.4.
– Nivel MEDIO: mp.if.4 + R1.
– Nivel ALTO: mp.if.4 + R1.

5.1.5 Protección frente a incendios [mp.if.5].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	aplica	aplica	aplica

Requisitos.

– [mp.if.5.1] Los locales donde se ubiquen los sistemas de información y sus componentes esenciales se protegerán frente a incendios atendiendo, al menos, a la normativa industrial de aplicación.

Aplicación de la medida (por disponibilidad).

– Nivel BAJO: mp.if.5.
– Nivel MEDIO: mp.if.5.
– Nivel ALTO: mp.if.5.

5.1.6 Protección frente a inundaciones [mp.if.6].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	n.a.	aplica	aplica

Requisitos.

– [mp.if.6.1] Los locales donde se ubiquen los sistemas de información y sus componentes esenciales se protegerán frente a incidentes causados por el agua.

Aplicación de la medida (por disponibilidad).

– Nivel BAJO: no aplica.
– Nivel MEDIO: mp.if.6.
– Nivel ALTO: mp.if.6.

5.1.7 Registro de entrada y salida de equipamiento [mp.if.7].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

– [mp.if.7.1] Se llevará un registro pormenorizado de cualquier entrada y salida de equipamiento esencial, incluyendo la identificación de la persona que autoriza el movimiento.

Aplicación de la medida.

– Categoría BÁSICA: mp.if.7.
– Categoría MEDIA: mp.if.7.
– Categoría ALTA: mp.if.7.

5.2 Gestión del personal [mp.per].

5.2.1 Caracterización del puesto de trabajo [mp.per.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	aplica	aplica

Requisitos.

– [mp.per.1.1] Para cada puesto de trabajo, relacionado directamente con el manejo de información o servicios, se definirán las responsabilidades en materia de seguridad, que estarán basadas en el análisis de riesgos.
– [mp.per.1.2] Se definirán los requisitos que deben satisfacer las personas que vayan a ocupar el puesto de trabajo, en particular, en términos de confidencialidad. Dichos requisitos se tendrán en cuenta en la selección de la persona que vaya a ocupar el puesto, incluyendo la verificación de sus antecedentes laborales, formación y otras referencias, de conformidad con el ordenamiento jurídico y el respeto a los derechos fundamentales.

Refuerzo R1-Habilitación Personal de Seguridad.

– [mp.per.1.r1.1] Los administradores de seguridad/sistema tendrán una Habilitación Personal de Seguridad (HPS) otorgada por la autoridad competente, como consecuencia de los resultados del análisis de riesgos previo o como requisito de seguridad de un sistema específico.

Aplicación de la medida.

– Categoría BÁSICA: no aplica.
– Categoría MEDIA: mp.per.1.
– Categoría ALTA: mp.per.1.

5.2.2 Deberes y obligaciones [mp.per.2].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+ R1

Requisitos.

Se informará a cada persona que trabaje en el sistema de los deberes y responsabilidades de su puesto de trabajo en materia de seguridad, contemplando:

– [mp.per.2.1] Las medidas disciplinarias a que haya lugar.
– [mp.per.2.2] Contemplando tanto el periodo durante el cual se desempeña el puesto, como las obligaciones en caso de término de la asignación, o traslado a otro puesto de trabajo.
– [mp.per.2.3] El deber de confidencialidad respecto de los datos a los que tenga acceso, tanto durante el periodo que esté adscrito al puesto de trabajo, como posteriormente a su terminación.
– [mp.per.2.4] En caso de personal contratado a través de un tercero:

• [mp.per.2.4.1] Se establecerán los deberes y obligaciones de cada parte y del personal contratado.
• [mp.per.2.4.2] Se establecerá el procedimiento de resolución de incidentes relacionados con el incumplimiento de las obligaciones.

Refuerzo R1-Confirmación expresa.

– [mp.per.2.r1.1] Se ha de obtener la confirmación expresa de que los usuarios conocen las instrucciones de seguridad necesarias y obligatorias y su aceptación, así como los procedimientos necesarios para llevarlas a cabo de manera adecuada.

Aplicación de la medida.

– Categoría BÁSICA: mp.per.2.
– Categoría MEDIA: mp.per.2 + R1.
– Categoría ALTA: mp.per.2 + R1.

5.2.3 Concienciación [mp.per.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

Se realizarán las acciones necesarias para concienciar regularmente al personal acerca de su papel y responsabilidad para que la seguridad del sistema alcance los niveles exigidos. En particular, se recordará periódicamente:

– [mp.per.3.1] La normativa de seguridad relativa al buen uso de los equipos o sistemas y las técnicas de ingeniería social más habituales.
– [mp.per.3.2] La identificación de incidentes, actividades o comportamientos sospechosos que deban ser reportados para su tratamiento por personal especializado.
– [mp.per.3.3] El procedimiento para informar sobre incidentes de seguridad, sean reales o falsas alarmas.

Aplicación de la medida.

– Categoría BÁSICA: mp.per.3.
– Categoría MEDIA: mp.per.3.
– Categoría ALTA: mp.per.3.

5.2.4 Formación [mp.per.4].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

– [mp.per.4.1] Se formará regularmente al personal en aquellas materias relativas a seguridad de la información que requiera el desempeño de sus funciones, en particular en lo relativo a:

a) Configuración de sistemas.
b) Detección y reacción ante incidentes.
c) Gestión de la información en cualquier soporte en el que se encuentre. Se cubrirán al menos las siguientes actividades: almacenamiento, transferencia, copias, distribución y destrucción.

Además, se evaluará la eficacia de las acciones formativas llevadas a cabo.

Aplicación de la medida.

– Categoría BÁSICA: mp.per.4.
– Categoría MEDIA: mp.per.4.
– Categoría ALTA: mp.per.4.

5.3 Protección de los equipos [mp.eq].

5.3.1 Puesto de trabajo despejado [mp.eq.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+ R1

Requisitos.

– [mp.eq.1.1] Los puestos de trabajo permanecerán despejados, sin que exista material distinto del necesario en cada momento.

Refuerzo R1-Almacenamiento del material.

– [mp.eq.1.r1.1] Una vez usado, y siempre que sea factible, el material se almacenará en lugar cerrado.

Aplicación de la medida.

– Categoría BÁSICA: mp.eq.1.
– Categoría MEDIA: mp.eq.1 + R1.
– Categoría ALTA: mp.eq.1 + R1.

5.3.2 Bloqueo de puesto de trabajo [mp.eq.2].

dimensiones	A		
nivel	BAJO	MEDIO	ALTO
	n.a.	aplica	+ R1

Requisitos.

– [mp.eq.2.1] El puesto de trabajo se bloqueará al cabo de un tiempo prudencial de inactividad, requiriendo una nueva autenticación del usuario para reanudar la actividad en curso.

Refuerzo R1-Cierre de sesiones.

– [mp.eq.2.r1.1] Pasado un cierto tiempo, superior al anterior, se cancelarán las sesiones abiertas desde dicho puesto de trabajo.

Una Guía CCN-STIC concretará la implementación de la configuración de seguridad adaptada a la categorización del sistema o perfil de cumplimiento asociado.

Aplicación de la medida (por autenticidad).

– Nivel BAJO: no aplica.
– Nivel MEDIO: mp.eq.2.
– Nivel ALTO: mp.eq.2 + R1.

5.3.3 Protección de dispositivos portátiles [mp.eq.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	+R1+R2

Requisitos.

Los equipos (ordenadores portátiles, tabletas, etc.) que sean susceptibles de salir de las instalaciones de la organización y no puedan beneficiarse de la protección física correspondiente, con un riesgo manifiesto de pérdida o robo, serán protegidos adecuadamente.
Sin perjuicio de las medidas generales que les afecten, se adoptarán las siguientes:

– [mp.eq.3.1] Se llevará un inventario de dispositivos portátiles junto con una identificación de la persona responsable de cada uno de ellos y un control regular de que está positivamente bajo su control.
– [mp.eq.3.2] Se establecerá un procedimiento operativo de seguridad para informar al servicio de gestión de incidentes de pérdidas o sustracciones.

– [mp.eq.3.3] Cuando un dispositivo portátil se conecte remotamente a través de redes que no están bajo el estricto control de la organización, el ámbito de operación del servidor limitará la información y los servicios accesibles a los mínimos imprescindibles, requiriendo autorización previa de los responsables de la información y los servicios afectados. Este punto es de aplicación a conexiones a través de internet y otras redes que no sean de confianza.

– [mp.eq.3.4] Se evitará, en la medida de lo posible, que el dispositivo portátil contenga claves de acceso remoto a la organización que no sean imprescindibles. Se considerarán claves de acceso remoto aquellas que sean capaces de habilitar un acceso a otros equipos de la organización u otras de naturaleza análoga.

Refuerzo R1– Cifrado del disco.

– [mp.eq.3.r1.1] Se protegerá el dispositivo portátil mediante cifrado del disco duro cuando el nivel de confidencialidad de la información almacenada en el mismo sea de nivel MEDIO.

Refuerzo R2– Entornos protegidos.

– [mp.eq.3.r2.1] El uso de dispositivos portátiles fuera de las instalaciones de la organización se restringirá a entornos protegidos, donde el acceso sea controlado y a salvo de hurtos y miradas indiscretas.

Aplicación de la medida.

– Categoría BÁSICA: mp.eq.3.
– Categoría MEDIA: mp.eq.3.
– Categoría ALTA: mp.eq.3 + R1 + R2.

5.3.4 Otros dispositivos conectados a la red [mp.eq.4].

dimensiones	C		
nivel	BAJO	MEDIO	ALTO
	aplica	+ R1	+ R1

Esta medida afecta a todo tipo de dispositivos conectados a la red y que puedan tener en algún momento acceso a la información, tales como:

a) Dispositivos multifunción: impresoras, escáneres, etc.
b) Dispositivos multimedia: proyectores, altavoces inteligentes, etc.
c) Dispositivos internet de las cosas, en inglés *Internet of Things* (*IoT*).
d) Dispositivos de invitados y los personales de los propios empleados, en inglés *Bring Your Own Device* (BYOD).
e) Otros.

Requisitos.

– [mp.eq.4.1] Los dispositivos presentes en el sistema deberán contar con una configuración de seguridad adecuada de manera que se garantice el control del flujo definido de entrada y salida de la información.

– [mp.eq.4.2] Los dispositivos presentes en la red que dispongan de algún tipo de almacenamiento temporal o permanente de información proporcionarán la funcionalidad necesaria para eliminar información de soportes de información. (Ver [mp.si.5]).

Refuerzo R1-Productos certificados.

– [mp.eq.4.r1.1] Se usarán, cuando sea posible, productos o servicios que cumplan lo establecido en [op.pl.5].

Refuerzo R2-Control de dispositivos conectados a la red.

– [mp.eq.4.r2.1] Se dispondrá de soluciones que permitan visualizar los dispositivos presentes en la red, controlar su conexión/desconexión a la misma y verificar su configuración de seguridad.

Aplicación de la medida (por confidencialidad).

– Nivel BAJO: mp.eq.4.
– Nivel MEDIO: mp.eq.4 + R1.
– Nivel ALTO: mp.eq.4+ R1.

5.4 Protección de las comunicaciones [mp.com].

5.4.1 Perímetro seguro [mp.com.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

– [mp.com.1.1] Se dispondrá de un sistema de protección perimetral que separe la red interna del exterior. Todo el tráfico deberá atravesar dicho sistema.
– [mp.com.1.2] Todos los flujos de información a través del perímetro deben estar autorizados previamente.

La Instrucción Técnica de Seguridad de Interconexión de Sistemas de Información determinará los requisitos establecidos en el perímetro que han de cumplir todos los componentes del sistema en función de la categoría.

Aplicación de la medida.

– Categoría BÁSICA: mp.com.1.
– Categoría MEDIA: mp.com.1.
– Categoría ALTA: mp.com.1.

5.4.2 Protección de la confidencialidad [mp.com.2].

dimensiones	C		
nivel	BAJO	MEDIO	ALTO
	aplica	+ R1	+R1+R2+R3

Requisitos.

– [mp.com.2.1] Se emplearán redes privadas virtuales cifradas cuando la comunicación discurra por redes fuera del propio dominio de seguridad.

Refuerzo R1-Algoritmos y parámetros autorizados.

– [mp.com.2.r1.1] Se emplearán algoritmos y parámetros autorizados por el CCN.

Refuerzo R2-Dispositivos hardware.

– [mp.com.2.r2.1] Se emplearán, dispositivos hardware en el establecimiento y utilización de la red privada virtual.

Refuerzo R3-Productos certificados.

– [mp.com.2.r3.1] Se usarán productos o servicios que cumplan lo establecido en [op.pl.5].

Refuerzo R4-Cifradores.

– [mp.com.2.r4.1] Se emplearán cifradores que cumplan con los requisitos establecidos en la guía CCN-STIC que sea de aplicación.

Refuerzo R5-Cifrado de información especialmente sensible.

– [mp.com.2.r5.1] Se cifrará toda la información transmitida.

Aplicación de la medida (por confidencialidad).

– Nivel BAJO: mp.com.2.

– Nivel MEDIO: mp.com.2 + R1.
– Nivel ALTO: mp.com.2 + R1 + R2+ R3.

5.4.3 Protección de la integridad y de la autenticidad [mp.com.3].

dimensiones	I A		
nivel	BAJO	MEDIO	ALTO
	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4

Requisitos.

– [mp.com.3.1] En comunicaciones con puntos exteriores al dominio propio de seguridad, se asegurará la autenticidad del otro extremo del canal de comunicación antes de intercambiar información. (Ver [op.acc.5]).
– [mp.com.3.2] Se prevendrán ataques activos garantizando que al ser detectados se activarán los procedimientos previstos de tratamiento del incidente. Se considerarán ataques activos:

a) La alteración de la información en tránsito.
b) La inyección de información espuria.
c) El secuestro de la sesión por una tercera parte.

– [mp.com.3.3] Se aceptará cualquier mecanismo de identificación y autenticación de los previstos en el ordenamiento jurídico y en la normativa de aplicación.

Refuerzo R1-Redes privadas virtuales.

– [mp.com.3.r1.1] Se emplearán redes privadas virtuales cifradas cuando la comunicación discurra por redes fuera del propio dominio de seguridad.

Refuerzo R2-Algoritmos y parámetros autorizados.

– [mp.com.3.r2.1] Se emplearán algoritmos y parámetros autorizados por el CCN.

Refuerzo R3-Dispositivos hardware.

– [mp.com.3.r3.1] Se recomienda emplear dispositivos hardware en el establecimiento y utilización de la red privada virtual.

Refuerzo R4-Productos certificados.

– [mp.com.3.r4.1] Se emplearán productos certificados conforme a lo establecido en [op.pl.5].

Refuerzo R5-Cifradores.

– [mp.com.3.r5.1] Se emplearán cifradores que cumplan con los requisitos establecidos en la guía CCN-STIC que sea de aplicación.

Aplicación de la medida (por integridad y autenticidad).

– Nivel BAJO: mp.com.3.
– Nivel MEDIO: mp.com.3 + R1 + R2.
– Nivel ALTO: mp.com.3 + R1 + R2 + R3 + R4.

5.4.4 Separación de flujos de información en la red [mp.com.4].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	+[R1oR2oR3]	+[R2oR3]+R4

La segmentación acota el acceso a la información y, consiguientemente, la propagación de los incidentes de seguridad, que quedan restringidos al entorno donde ocurren.
Cuando la transmisión de información por la red se restringe a ciertos segmentos, se acota el acceso a la información y los incidentes de seguridad quedan encapsulados en su segmento.

Requisitos.

Los flujos de información se separarán en segmentos de forma que:

– [mp.com.4.1] El tráfico por la red se segregará para que cada equipo solamente tenga acceso a la información que necesita.
– [mp.com.4.2] Si se emplean comunicaciones inalámbricas, será en un segmento separado.

Refuerzo R1-Segmentación lógica básica.

– [mp.com.4.r1.1] Los segmentos de red se implementarán por medio de redes de área local virtuales (*Virtual Local Area Network, VLAN*).
– [mp.com.4.r1.2] La red que conforma el sistema deberá segregarse en distintas subredes contemplando como mínimo:

• Usuarios.
• Servicios.
• Administración.

Refuerzo R2-Segmentación lógica avanzada.

– [mp.com.4.r2.1] Los segmentos de red se implementarán por medio de redes privadas virtuales (*Virtual Private Network, VPN*).

Refuerzo R3-Segmentación física.

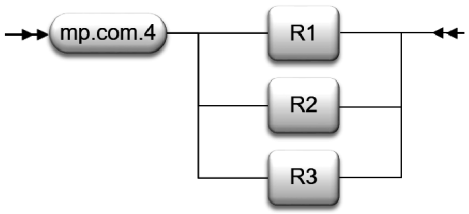
– [mp.com.4.r3.1] Los segmentos de red se implementarán con medios físicos separados.

Refuerzo R4-Puntos de interconexión.

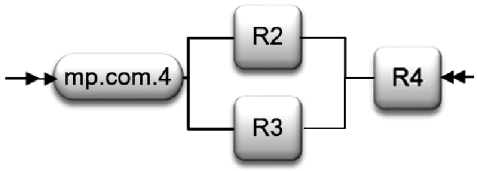
– [mp.com.4.r4.1] Control de entrada de los usuarios que llegan a cada segmento y control de entrada y salida de la información disponible en cada segmento.
– [mp.com.4.r4.2] El punto de interconexión estará particularmente asegurado, mantenido y monitorizado, (como en [mp.com.1]).

Aplicación de la medida.

– Categoría BÁSICA: no aplica.
– Categoría MEDIA: mp.com.4+ [R1o R2 o R3].



– Categoría ALTA: mp.com.4+[R2 o R3] + R4.



5.5 Protección de los soportes de información [mp.si].

5.5.1 Marcado de soportes [mp.si.1].

dimensiones	C		
nivel	BAJO	MEDIO	ALTO
	n.a.	aplica	aplica

Requisitos.

– [mp.si.1.1] Los soportes de información (papel impreso, documentos electrónicos, contenidos multimedia -vídeos, cursos, presentaciones- etc.) que contengan información que según [mp.info.2] deba protegerse con medidas de seguridad específicas, llevarán las marcas o metadatos correspondientes que indiquen el nivel de seguridad de la información contenida de mayor calificación.

Refuerzo R1-Marca de agua digital.

– [mp.si.1.r1.1] La política de seguridad de la organización definirá marcas de agua para asegurar el uso adecuado de la información que se maneja.
– [mp.si.1.r1.2] Los soportes de información digital (documentos electrónicos, material multimedia, etc.) podrán incluir una marca de agua según la política de seguridad.
– [mp.si.1.r1.3] Los equipos o dispositivos a través de los que se accede a aplicaciones, escritorios remotos o virtuales, datos, etc., presentarán una marca de agua en pantalla según la política de seguridad.

Aplicación de la medida (por confidencialidad).

– Nivel BAJO: no aplica.
– Nivel MEDIO: mp.si.1.
– Nivel ALTO: mp.si.1.

5.5.2 Criptografía [mp.si.2].

dimensiones	C I		
nivel	BAJO	MEDIO	ALTO
	n.a.	aplica	+ R1 + R2

Esta medida se aplica, en particular, a todos los dispositivos removibles cuando salen de un área controlada. Se entenderán por dispositivos removibles, los CD, DVD, discos extraíbles, *pendrives*, memorias USB u otros de naturaleza análoga.

Requisitos.

– [mp.si.2.1] Se usarán mecanismos criptográficos que garanticen la confidencialidad y la integridad de la información contenida.
– [mp.si.2.2] Se emplearán algoritmos y parámetros autorizados por el CCN.

Refuerzo R1– Productos certificados.

– [mp.si.2.r1.1] Se emplearán productos certificados conforme a lo establecido en [op.pl.5].

Refuerzo R2-Copias de seguridad.

– [mp.si.2.r2.1] Las copias se seguridad se cifrarán utilizando algoritmos y parámetros autorizados por el CCN.

Aplicación de la medida (por confidencialidad e integridad).

– Nivel BAJO: no aplica.
– Nivel MEDIO: mp.si.2.
– Nivel ALTO: mp.si.2 + R1 + R2.

5.5.3 Custodia [mp.si.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA

	aplica	aplica	aplica

Requisitos.

– [mp.si.3.1] Se aplicará la debida diligencia y control a los soportes de información que permanecen bajo la responsabilidad de la organización, garantizando el control de acceso con medidas físicas ([mp.if.1] y [mp.if.7]) o lógicas ([mp.si.2]).
– [mp.si.3.2] Se respetarán las exigencias de mantenimiento del fabricante, en especial, en lo referente a temperatura, humedad y otros agentes medioambientales.

Aplicación de la medida.

– Categoría BÁSICA: mp.si.3.
– Categoría MEDIA: mp.si.3.
– Categoría ALTA: mp.si.3.

5.5.4 Transporte [mp.si.4].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

El responsable del sistema garantizará que los dispositivos permanecen bajo control y que satisfacen sus requisitos de seguridad mientras están siendo desplazados de un lugar a otro, fuera de las zonas controladas por la organización.

Requisitos.

– [mp.si.4.1] Se dispondrá de un registro de entrada/salida que identifique al transportista que entrega/recibe el soporte.
– [mp.si.4.2] Se dispondrá de un procedimiento rutinario que coteje las salidas con las llegadas y levante las alarmas pertinentes cuando se detecte algún incidente.
– [mp.si.4.3] Se utilizarán los medios de protección criptográfica ([mp.si.2]) correspondientes al mayor nivel de seguridad de la información contenida.
– [mp.si.4.4] Se gestionarán las claves según [op.exp.10].

Aplicación de la medida.

– Categoría BÁSICA: mp.si.4.
– Categoría MEDIA: mp.si.4.
– Categoría ALTA: mp.si.4.

5.5.5 Borrado y destrucción [mp.si.5].

dimensiones	C		
nivel	BAJO	MEDIO	ALTO
	aplica	+ R1	+ R1

La medida de borrado y destrucción de soportes de información se aplicará a todo tipo de equipos y soportes susceptibles de almacenar información, incluyendo medios electrónicos y no electrónicos.

Requisitos.

– [mp.si.5.1] Los soportes que vayan a ser reutilizados para otra información o liberados a otra organización serán objeto del borrado seguro de su contenido que no permita su recuperación. Cuando la naturaleza del soporte no permita un borrado seguro, el soporte no podrá ser reutilizado en ningún otro sistema.

Las guías CCN-STIC del CCN precisarán los criterios para definir como seguro un mecanismo de borrado o de destrucción, en función de la sensibilidad de la información almacenada en el dispositivo.

Refuerzo R1-Productos certificados.

– [mp.si.5.r1.1] Se usarán productos o servicios que cumplan lo establecido en [op.pl.5].

Refuerzo R2 - Destrucción de soportes.

– [mp.si.5.r2.1] Una vez finalizado el ciclo de vida del soporte de información, deberá ser destruido de forma segura conforme a los criterios establecidos por el CCN.

Aplicación de la medida (por confidencialidad).

– Nivel BAJO: mp.si.5.
– Nivel MEDIO: mp.si.5 + R1.
– Nivel ALTO: mp.si.5 + R1.

5.6 Protección de las aplicaciones informáticas [mp.sw].

5.6.1 Desarrollo de aplicaciones [mp.sw.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	+R1+R2+R3+R4	+R1+R2+R3+R4

Requisitos.

– [mp.sw.1.1] El desarrollo de aplicaciones se realizará sobre un sistema diferente y separado del de producción, no debiendo existir herramientas o datos de desarrollo en el entorno de producción, ni datos de producción en el de desarrollo.

Refuerzo R1-Mínimo privilegio.

– [mp.sw.1.r1.1] Las aplicaciones se desarrollarán respetando el principio de mínimo privilegio, accediendo únicamente a los recursos imprescindibles para su función, y con los privilegios que sean indispensables.

Refuerzo R2-Metodología de desarrollo seguro.

– [mp.sw.1.r2.1] Se aplicará una metodología de desarrollo seguro reconocida que:

a) Tendrá en consideración los aspectos de seguridad a lo largo de todo el ciclo de vida.
b) Incluirá normas de programación segura, especialmente: control de asignación y liberación de memoria, desbordamiento de memoria (*overflow*).
c) Tratará específicamente los datos usados en pruebas.
d) Permitirá la inspección del código fuente.

Refuerzo R3-Seguridad desde el diseño.

– [mp.sw.1.r3.1] Los siguientes elementos serán parte integral del diseño del sistema:

a) Los mecanismos de identificación y autenticación.
b) Los mecanismos de protección de la información tratada.
c) La generación y tratamiento de pistas de auditoría.

Refuerzo R4-Datos de pruebas.

– [mp.sw.1.r4.1] Preferiblemente, las pruebas previas a la implantación o modificación de los sistemas de información no se realizarán con datos reales. En caso de que fuese necesario recurrir a datos reales se garantizará el nivel de seguridad correspondiente.

Refuerzo R5-Lista de componentes software.

– [mp.sw.1.r5.1] El desarrollador elaborará y mantendrá actualizada una relación formal de los componentes software de terceros empleados en la aplicación o producto. Se mantendrá un histórico de los componentes utilizados en las diferentes versiones del software. El contenido mínimo de la lista de componentes, que contendrá, al menos, la identificación del componente, el fabricante y la versión empleada, se concretará en una guía CCN-STIC del CCN.

Aplicación de la medida.

– Categoría BÁSICA: no aplica.
– Categoría MEDIA: mp.sw.1 + R1 + R2 + R3 + R4.
– Categoría ALTA: mp.sw.1 + R1 + R2 + R3 + R4.

5.6.2 Aceptación y puesta en servicio [mp.sw.2].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+ R1

Requisitos.

Antes de pasar a producción se comprobará el correcto funcionamiento de la aplicación.

– [mp.sw.2.1] Se comprobará que:

a) Se cumplen los criterios de aceptación en materia de seguridad.
b) No se deteriora la seguridad de otros componentes del servicio.

Refuerzo R1- Pruebas.

– [mp.sw.2.r1.1] Las pruebas se realizarán en un entorno aislado (pre-producción).

Refuerzo R2-Inspección de código fuente.

– [mp.sw.2.r2.1] Se realizará una auditoría de código fuente.

Aplicación de la medida.

– Categoría BÁSICA: mp.sw.2.
– Categoría MEDIA: mp.sw.2 + R1.
– Categoría ALTA: mp.sw.2 + R1.

5.7 Protección de la información [mp.info].

5.7.1 Datos personales [mp.info.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

– [mp.info.1.1] Cuando el sistema trate datos personales, el responsable de seguridad recogerá los requisitos de protección de datos que sean fijados por el responsable o por el encargado del tratamiento, contando con el asesoramiento del DPD, y que sean necesarios implementar en los sistemas de acuerdo a la naturaleza, alcance, contexto y fines del mismo, así como de los riesgos para los derechos y libertades de acuerdo a lo establecido en los artículos 24 y 32 del RGPD, y de acuerdo a la evaluación de impacto en la protección de datos, si se ha llevado a cabo.

Aplicación de la medida.

– Categoría BÁSICA: mp.info.1.
– Categoría MEDIA: mp.info.1.
– Categoría ALTA: mp.info.1.

5.7.2 Calificación de la información [mp.info.2].

dimensiones	C		
nivel	BAJO	MEDIO	ALTO
	n.a.	aplica	aplica

Requisitos.

– [mp.info.2.1] Para calificar la información se estará a lo establecido legalmente por las leyes y tratados internacionales de los que España es miembro y su normativa de aplicación cuando se trate de materias clasificadas. El valor a emplear en el caso de información de materias no clasificadas sería USO OFICIAL para información con algún tipo de restricción en su manejo por su sensibilidad y confidencialidad.

– [mp.info.2.2] La política de seguridad establecerá quién es el responsable de cada información manejada por el sistema.

– [mp.info.2.3] La política de seguridad recogerá, directa o indirectamente, los criterios que, en cada organización, determinarán el nivel de seguridad requerido, dentro del marco establecido en el artículo 40 y los criterios generales señalados en el anexo I.

– [mp.info.2.4] El responsable de cada información seguirá los criterios determinados en el apartado anterior para asignar a cada información el nivel de seguridad requerido, y será responsable de su documentación y aprobación formal.

– [mp.info.2.5] El responsable de cada información en cada momento tendrá en exclusiva la potestad de modificar el nivel de seguridad requerido, de acuerdo a los apartados anteriores.

Aplicación de la medida (por confidencialidad).

– Nivel BAJO: no aplica.
– Nivel MEDIO: mp.info.2.
– Nivel ALTO: mp.info.2.

5.7.3 Firma electrónica [mp.info.3].

dimensiones	I A		
nivel	BAJO	MEDIO	ALTO
	aplica	+R1+R2+R3	+ R1+R2+R3+R4

Requisitos.

– [mp.info.3.1] Se empleará cualquier tipo de firma electrónica de los previstos en el vigente ordenamiento jurídico, entre ellos, los sistemas de código seguro de verificación vinculados a la Administración Pública, órgano, organismo público o entidad de derecho público, en los términos y condiciones establecidos en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y en la Ley 40/2015, de 1 de octubre.

Refuerzo R1-Certificados cualificados.

– [mp.info.3.r1.1] Cuando se empleen sistemas de firma electrónica avanzada basados en certificados, estos serán cualificados.

Refuerzo R2-Algoritmos y parámetros autorizados.

– [mp.info.3.r2.1] Se emplearán algoritmos y parámetros autorizados por el CCN o por un esquema nacional o europeo que resulte de aplicación.

El CCN determinará los algoritmos criptográficos que hayan sido autorizados nominalmente para su uso en el Esquema Nacional de Seguridad conforme a la Instrucción Técnica de Seguridad Criptología de empleo en el ENS.

Refuerzo R3-Verificación y validación de firma.

– [mp.info.3.r3.1] Cuando proceda, se garantizará la verificación y validación de la firma electrónica durante el tiempo requerido por la actividad administrativa que aquélla soporte, sin perjuicio de que se pueda ampliar este período de acuerdo con lo que establezca la Política de Firma Electrónica y de Certificados que sea de aplicación. Para tal fin se adjuntará a la firma, o se referenciará, toda la información pertinente para su verificación y validación, incluyendo certificados o datos de verificación y validación.

Refuerzo R4-Firma electrónica avanzada basada en certificados cualificados.

– [mp.info.3.r4.1] Se usará firma electrónica avanzada basada en certificados cualificados complementada por un segundo factor del tipo «algo que se sabe» o «algo que se es».

Refuerzo R5-Firma electrónica cualificada.

– [mp.info.3.r5.1] Se usará firma electrónica cualificada, empleando productos certificados conforme a lo establecido en [op.pl.5].

Aplicación de la medida (por integridad y autenticidad).

– Nivel BAJO: mp.info.3.
– Nivel MEDIO: mp.info.3 + R1 + R2 + R3.
– Nivel ALTO: mp.info.3 + R1 + R2 + R3 + R4.

5.7.4 Sellos de tiempo [mp.info.4].

dimensiones	T		
nivel	BAJO	MEDIO	ALTO
	n.a.	n.a.	aplica

Requisitos.

La utilización de sellos de tiempo exigirá adoptar las siguientes cautelas:

– [mp.info.4.1] Los sellos de tiempo se aplicarán a aquella información que sea susceptible de ser utilizada como evidencia electrónica en el futuro.
– [mp.info.4.2] Los datos pertinentes para la verificación posterior de la fecha serán tratados con la misma seguridad que la información fechada a efectos de disponibilidad, integridad y confidencialidad.
– [mp.info.4.3] Se renovarán regularmente los sellos de tiempo hasta que la información protegida ya no sea requerida por el proceso administrativo al que da soporte, en su caso.
– [mp.info.4.4] Se emplearán "sellos cualificados de tiempo electrónicos" atendiendo a lo dispuesto en el Reglamento (UE) n.º 910/2014 y normativa de desarrollo.

Refuerzo R1-Productos certificados.

– [mp.info.4.r1.1.] Se utilizarán productos certificados según [op.pl.5].
– [mp.info.4.r1.2] Se asignará una fecha y hora a un documento electrónico, conforme a lo establecido en la guía CCN-STIC Criptología de empleo en el ENS.

Aplicación de la medida (por trazabilidad).

– Nivel BAJO: no aplica.
– Nivel MEDIO: no aplica.
– Nivel ALTO: mp.info.4.

5.7.5 Limpieza de documentos [mp.info.5].

dimensiones	C		
nivel	BAJO	MEDIO	ALTO
	aplica	aplica	aplica

Requisitos.

– [mp.info.5.1] En el proceso de limpieza de documentos, se retirará de estos toda la información adicional contenida en campos ocultos, metadatos, comentarios o revisiones anteriores, salvo cuando dicha información sea pertinente para el receptor del documento.

Esta medida es especialmente relevante cuando el documento se difunde ampliamente, como ocurre cuando se ofrece al público en un servidor web u otro tipo de repositorio de información.

Aplicación de la medida (por confidencialidad).

– Nivel BAJO: mp.info.5.
– Nivel MEDIO: mp.info.5.
– Nivel ALTO: mp.info.5.

5.7.6 Copias de seguridad [mp.info.6].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	aplica	+ R1	+ R1 + R2

Requisitos.

– [mp.info.6.1] Se realizarán copias de seguridad que permitan recuperar datos perdidos, accidental o intencionadamente. La periodicidad y los plazos de retención de estas copias de seguridad se determinarán en la normativa interna de la organización relativa a copias de seguridad.
– [mp.info.6.2] Los procedimientos de respaldo establecidos indicarán:

a) Frecuencia de las copias.
b) Requisitos de almacenamiento en el propio lugar.
c) Requisitos de almacenamiento en otros lugares.
d) Controles para el acceso autorizado a las copias de respaldo.

Refuerzo R1-Pruebas de recuperación.

– [mp.info.6.r1.1] Los procedimientos de copia de seguridad y restauración deben probarse regularmente. Su frecuencia dependerá de la criticidad de los datos y del impacto que cause la falta de disponibilidad.

Refuerzo R2-Protección de las copias de seguridad.

– [mp.info.6.r2.1] Al menos, una de las copias de seguridad se almacenará de forma separada en lugar diferente, de tal manera que un incidente no pueda afectar tanto al repositorio original como a la copia simultáneamente.
– Nivel BAJO: mp.info.6.
– Nivel MEDIO: mp.info.6+ R1.
– Nivel ALTO: mp.info.6+ R1 + R2.

5.8 Protección de los servicios [mp.s].

5.8.1 Protección del correo electrónico [mp.s.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

El correo electrónico se protegerá frente a las amenazas que le son propias, actuando del siguiente modo:

– [mp.s.1.1] La información distribuida por medio de correo electrónico se protegerá, tanto en el cuerpo de los mensajes como en los anexos.
– [mp.s.1.2] Se protegerá la información de encaminamiento de mensajes y establecimiento de conexiones.

Se protegerá a la organización frente a problemas que se materializan por medio del correo electrónico, en concreto:

– [mp.s.1.3] Correo no solicitado, en su expresión inglesa «*spam*».
– [mp.s.1.4] Código dañino, constituidos por virus, gusanos, troyanos, espías, u otros de naturaleza análoga.
– [mp.s.1.5] Código móvil de tipo micro-aplicación, en su expresión inglesa «*applet*».

Se establecerán normas de uso del correo electrónico para el personal. (Ver [org.2]). Estas normas de uso contendrán:

– [mp.s.1.6] Limitaciones al uso como soporte de comunicaciones privadas.
– [mp.s.1.7] Actividades de concienciación y formación relativas al uso del correo electrónico.

Aplicación de la medida.

– Categoría BÁSICA: mp.s.1.
– Categoría MEDIA: mp.s.1.
– Categoría ALTA: mp.s.1.

5.8.2 Protección de servicios y aplicaciones web [mp.s.2].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	+[R1oR2]	+[R1oR2]	+R2+R3

Requisitos.

Los sistemas que prestan servicios *web* deberán ser protegidos frente a las siguientes amenazas:

– [mp.s.2.1] Cuando la información requiera control de acceso se garantizará la imposibilidad de acceder a la información obviando la autenticación, en particular, tomando medidas en los siguientes aspectos:

a) Se evitará que el servidor ofrezca acceso a los documentos por vías alternativas al protocolo determinado.
b) Se prevendrán ataques de manipulación del localizador uniforme de recursos (*Uniform Resource Locator, URL*).
c) Se prevendrán ataques de manipulación de fragmentos de información que se almacena en el disco duro del visitante de una página web a través de su navegador, a petición del servidor de la página, conocido en terminología inglesa como *cookies*.
d) Se prevendrán ataques de inyección de código.

– [mp.s.2.2] Se prevendrán intentos de escalado de privilegios.
– [mp.s.2.3] Se prevendrán ataques *de cross site scripting*.

Refuerzo R1-Auditorías de seguridad.

– [mp.s.2.r1.1] Se realizarán auditorías continuas de seguridad de «caja negra» sobre las aplicaciones web durante la fase de desarrollo y antes de la fase de producción.
– [mp.s.2.r1.2] La frecuencia de estas auditorías de seguridad quedará definida en el procedimiento de auditoría.

Refuerzo R2-Auditorías de seguridad avanzada.

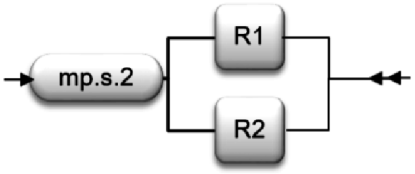
– [mp.s.2.r2.1] Se realizarán auditorías de seguridad de «caja blanca» sobre las aplicaciones web durante la fase de desarrollo.
– [mp.s.2.r2.2] Se emplearán metodologías definidas y herramientas automáticas de detección de vulnerabilidades en la realización de las auditorías de seguridad sobre las aplicaciones web.
– [mp.s.2.r2.3] Una vez finalizada una auditoría de seguridad, se analizarán los resultados y se solventarán las vulnerabilidades encontradas mediante los procedimientos definidos [op.exp.5].

Refuerzo R3-Protección de las cachés.

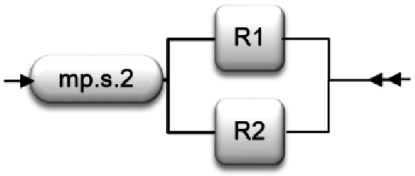
– [mp.s.2.r3.1] Se prevendrán ataques de manipulación de programas o dispositivos que realizan una acción en representación de otros, conocidos en terminología inglesa como "*proxies*" y, sistemas especiales de almacenamiento de alta velocidad, conocidos en terminología inglesa como "*cachés*".

Aplicación de la medida.

– Categoría BÁSICA: mp.s.2 + [R1 o R2].



– Categoría MEDIA: mp.s.2 + [R1 o R2].



– Categoría ALTA: mp.s.2 + R2 + R3.

5.8.3 Protección de la navegación web [mp.s.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	+ R1

Requisitos.

El acceso de los usuarios internos a la navegación por internet se protegerá frente a las amenazas que le son propias, actuando del siguiente modo:

– [mp.s.3.1] Se establecerá una normativa de utilización, definiendo el uso que se autoriza y las limitaciones de uso personal. En particular, se concretará el uso permitido de conexiones cifradas.
– [mp.s.3.2] Se llevarán a cabo regularmente actividades de concienciación sobre higiene en la navegación web, fomentando el uso seguro y alertando de usos incorrectos.
– [mp.s.3.3] Se formará al personal encargado de la administración del sistema en monitorización del servicio y respuesta a incidentes.
– [mp.s.3.4] Se protegerá la información de resolución de direcciones web y de establecimiento de conexiones.
– [mp.s.3.5] Se protegerá a la organización en general y al puesto de trabajo en particular frente a problemas que se materializan vía navegación web.
– [mp.s.3.6] Se protegerá contra la actuación de programas dañinos tales como páginas activas, descargas de código ejecutable, etc., previniendo la exposición del sistema a vectores de ataque del tipo *spyware*, *ransomware*, etc.
– [mp.s.3.7] Se establecerá una política ejecutiva de control de cookies, en particular, para evitar la contaminación entre uso personal y uso organizativo.

Refuerzo R1 - Monitorización.

– [mp.s.3.r1.1] Se registrará el uso de la navegación web, estableciendo los elementos que se registran, el periodo de retención de estos registros y el uso que el organismo prevé hacer de ellos.
– [mp.s.3.r1.2] Se establecerá una función para la ruptura de canales cifrados a fin de inspeccionar su contenido, indicando qué se analiza, qué se registra, durante cuánto tiempo se retienen los registros y qué uso prevé hacer el organismo de estas inspecciones. Todo

ello sin perjuicio de que se puedan autorizar accesos cifrados singulares a destinos de confianza.

– [mp.s.3.r1.3] Se establecerá una lista negra de destinos vetados.

Refuerzo R2-Destinos autorizados.

– [mp.s.3.r2.1] Se establecerá una lista blanca de destinos accesibles. Todo acceso fuera de los lugares señalados en la lista blanca estará vetado, salvo autorización singular expresa.

Aplicación de la medida.

– Categoría BÁSICA: mp.s.3.
– Categoría MEDIA: mp.s.3.
– Categoría ALTA: mp.s.3 + R1.

5.8.4 Protección frente a la denegación de servicio [mp.s.4].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	n.a.	aplica	+ R1

Requisitos.

Se establecerán medidas preventivas frente a ataques de denegación de servicio y denegación de servicio distribuido (*Denial of Service, DoS y Distributed Denial of Service, DDoS*). Para ello:

– [mp.s 4.1] Se planificará y dotará al sistema de capacidad suficiente para atender con holgura a la carga prevista.

– [mp.s.4.2] Se desplegarán tecnologías para prevenir los ataques conocidos.

Refuerzo R1-Detección y reacción.

– [mp.s.4.r1.1] Se establecerá un sistema de detección y tratamiento de ataques de denegación de servicio (DoS y DDoS).

– [mp.s. 4.r1.2] Se establecerán procedimientos de reacción a los ataques, incluyendo la comunicación con el proveedor de comunicaciones.

Refuerzo R2-Ataques propios.

– [mp.s.4.r2.1] Se detectará y se evitará el lanzamiento de ataques desde las propias instalaciones perjudicando a terceros.

Aplicación de la medida (por disponibilidad).

– Nivel BAJO: no aplica.
– Nivel MEDIO: mp.s.4.
– Nivel ALTO: mp.s.4+ R1.

6. Valoración de la implantación de las medidas de seguridad

Es habitual el empleo de niveles de madurez para caracterizar la implementación de un proceso. El modelo de madurez de capacidad (*Capability Maturity Model, CMM)* permite describir las características que hacen un proceso efectivo, midiendo el grado o nivel de profesionalización de la actividad.

Un proceso es una colección de actividades o tareas relacionadas y estructuradas que, en una secuencia específica, proporciona un servicio para la organización.

Para la valoración de la implantación de las medidas de seguridad, estás se analizarán como procesos y se estimará su nivel de madurez usando el modelo de madurez de capacidad (CMM).

Se identifican cinco "niveles de madurez", de modo que una organización que tenga institucionalizadas todas las prácticas incluidas en un nivel y sus inferiores, se considera que ha alcanzado ese nivel de madurez:

a) L0-Inexistente.

No existe un proceso que soporte el servicio requerido.

b) L1 - Inicial. Ad hoc.

Las organizaciones en este nivel no disponen de un ambiente estable para la prestación del servicio requerido. Aunque se utilicen técnicas correctas de ingeniería, los esfuerzos se ven minados por falta de planificación. El éxito de los proyectos se basa la mayoría de las veces en el esfuerzo personal, aunque a menudo se producen fracasos y casi siempre retrasos y sobrecostes. El resultado es impredecible. A menudo las soluciones se implementan de forma reactiva a los incidentes.

Los procedimientos de trabajo, cuando existen, son informales, incompletos y no se aplican de forma sistemática.

c) L2-Reproducible, pero intuitivo.

En este nivel las organizaciones disponen de unas prácticas institucionalizadas de gestión, existen unas métricas básicas y un razonable seguimiento de la calidad.

Existen procedimientos de trabajo, pero no están suficientemente documentados o no cubren todos los aspectos requeridos.

d) L3-Proceso definido.

Además de una buena gestión, a este nivel las organizaciones disponen de normativa y procedimientos detallados y documentados de coordinación entre grupos, formación del personal, técnicas de ingeniería, etc.

e) L4-Gestionado y medible.

Se caracteriza porque las organizaciones disponen de un conjunto de métricas de efectividad y eficiencia, que se usan de modo sistemático para la toma de decisiones y la gestión de riesgos. El servicio resultante es de alta calidad.

f) L5 - Optimizado.

La organización completa está volcada en la mejora continua de los procesos. Se hace uso intensivo de las métricas y se gestiona el proceso de innovación.

Para cada medida de seguridad que sea de aplicación al sistema de información se exigirá un determinado nivel de madurez. Los niveles mínimos de madurez requeridos por el ENS en función de la categoría del sistema son:

Categoría del sistema	Nivel mínimo de madurez requerido
BÁSICA	L2-Reproducible, pero intuitivo.
MEDIA	L3-Proceso definido.
ALTA	L4-Gestionado y medible.

7. Desarrollo y complemento de las medidas de seguridad

Las medidas de seguridad se desarrollarán y complementarán según lo establecido en la disposición final segunda.

8. Interpretación

La interpretación de este anexo se realizará según el sentido propio de sus palabras, en relación con el contexto, antecedentes históricos y legislativos, entre los que figura lo dispuesto en las instrucciones técnicas de seguridad y en las guías CCN-STIC que sean de aplicación a la implementación y a los diversos escenarios de aplicación tales como sedes electrónicas, servicios de validación de certificados electrónicos, servicios de fechado electrónico y validación de documentos fechados, atendiendo el espíritu y finalidad de aquellas.

ANEXO III

Auditoría de la seguridad

1. Objeto de la auditoría

1.1 La seguridad de los sistemas de información de una organización será auditada en los siguientes términos, al objeto de constatar:

a) Que la política de seguridad define los roles y funciones de los responsables del sistema, la información, los servicios y la seguridad del sistema de información.
b) Que existen procedimientos para resolución de conflictos entre dichos responsables.
c) Que se han designado personas para dichos roles a la luz del principio de «diferenciación de responsabilidades».
d) Que se ha realizado un análisis de riesgos, con revisión y aprobación anual.
e) Que se cumplen las recomendaciones de protección descritas en el anexo II, sobre Medidas de Seguridad, en función de las condiciones de aplicación en cada caso.
f) Que existe un sistema de gestión de la seguridad de la información, documentado y con un proceso regular de aprobación por la dirección, tomando como base la Declaración de Aplicabilidad regulada en el artículo 28 de este real decreto.

1.2 La auditoría se basará en la existencia de evidencias que permitan sustentar objetivamente el cumplimiento de los siguientes puntos:

a) Documentación de los procedimientos.
b) Registro de incidentes.
c) Examen del personal afectado: conocimiento y praxis de las medidas que le afectan.
d) Productos certificados. Se considerará evidencia suficiente el empleo de productos que satisfagan lo establecido en artículo 19 «Adquisición de productos de seguridad y contratación de servicios de seguridad».

1.3 Se dispondrá de un programa o plan de auditorías documentado. Las actividades de auditoría que impliquen comprobaciones en los sistemas operativos deberán ser planificadas y acordadas previamente.

2. Niveles de auditoría

Los niveles de auditoría que se realizan a los sistemas de información serán los siguientes:

2.1 Auditoría a sistemas de categoría BÁSICA.

a) Los sistemas de información de categoría BÁSICA no necesitarán realizar una auditoría. Bastará una autoevaluación realizada por el mismo personal que administra el sistema de información o en quien éste delegue.
El resultado de la autoevaluación debe estar documentado, indicando si cada medida de seguridad está implantada y sujeta a revisión regular, así como las evidencias que sustentan la valoración anterior.
b) Los informes de autoevaluación serán analizados por el responsable de la seguridad competente, que elevará las conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.

2.2 Auditoría a sistemas de categoría MEDIA O ALTA.

a) El informe de auditoría dictaminará sobre el grado de cumplimiento de este real decreto e identificando los hallazgos de conformidad y no conformidad. Deberá, igualmente, incluir los criterios metodológicos de auditoría utilizados, el alcance y el objetivo de la auditoría, y los datos, hechos y observaciones en que se basen las conclusiones formuladas.
b) Los informes de auditoría serán analizados por el responsable de la seguridad competente, que presentará sus conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.

3. Interpretación

La interpretación de este anexo se realizará según el sentido propio de sus palabras, en relación con el contexto, antecedentes históricos y legislativos, entre los que figura lo dispuesto en la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los sistemas de información y en la guía CCN-STIC que sea de aplicación, atendiendo al espíritu y finalidad de aquellas.

ANEXO IV

Glosario

– Activo: componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

– Administrador del sistema/de la seguridad del sistema: persona encargada de la instalación y el mantenimiento de un sistema de información, implantando los procedimientos y la configuración de seguridad que se haya establecido en el marco de la política de seguridad del organismo.

– Análisis de riesgos: estudio de las consecuencias previsibles de un posible incidente de seguridad, considerando su impacto en la organización (en la protección de sus activos, en su misión, en su imagen o reputación, o en sus funciones) y la probabilidad de que ocurra.

– Área controlada: zona o área en la que una organización considera cumplidas las medidas de seguridad físicas y procedimentales requeridas para la protección de la información y los sistemas de información ubicados en ella.

– Arquitectura de seguridad: conjunto de elementos físicos y lógicos que forman parte de la arquitectura del sistema y cuyo objetivo es la protección de los activos dentro del sistema y en las interconexiones con otros sistemas.

– Auditoría de la seguridad: es un proceso sistemático, independiente y documentado que persigue la obtención de evidencias objetivas y su evaluación objetiva para determinar en qué medida se cumplen los criterios de auditoría en relación con la idoneidad de los controles de seguridad adoptados, el cumplimiento de la política de seguridad, las normas y los procedimientos operativos establecidos, y detectando desviaciones a los antedichos criterios.

– Autenticación: ratificación de la identidad de un usuario, proceso o dispositivo.

– Autenticación multifactor: exigencia de dos o más factores de autenticación para ratificar una autenticación como válida.

– Autenticador: algo, físico o inmaterial, que posee el usuario bajo su exclusivo control y que le distingue de otros usuarios.

– Autenticidad: propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

– Biometría (factor de autenticación): reconocimiento de los individuos en base a sus características biológicas o de comportamiento.

– Cadena de suministro: conjunto relacionado de recursos y procesos que comienza con la provisión de materias primas y se extiende a través de la entrega de productos o servicios al usuario final a través de los modos de transporte. Incluye a los proveedores (primer, segundo y tercer nivel), los almacenes de materia prima (directa o indirecta), las líneas de producción, los almacenes de productos terminados y los canales de distribución (mayoristas y minoristas), hasta llegar al cliente final.

– Categoría de seguridad de un sistema: es un grado, dentro de la escala Básica-Media-Alta, con el que se adjetiva un sistema de información a fin de seleccionar las medidas de seguridad necesarias para el mismo. La categoría de seguridad del sistema recoge la visión holística del conjunto de activos como un todo armónico, orientado a la prestación de unos servicios.

– Certificado de firma electrónica (factor de autenticación): una declaración electrónica que vincula los datos de validación de una firma con una persona física o jurídica y confirma, al menos, el nombre o el seudónimo de esa persona.

– Certificado cualificado de firma electrónica: un certificado de firma electrónica que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo I del Reglamento (UE) 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

– Ciberamenaza: amenaza a los sistemas y servicios presentes en el ciberespacio o alcanzables a través de éste.

– Ciberataque: cualquier conducta dolosa de individuos u organizaciones, conocidos o no, desarrollada a través del ciberespacio contra sistemas de información, con el propósito de sustraer, alterar, abusar, desestabilizar, inutilizar, destruir o eliminar activos.

– Ciberespacio: dominio global y dinámico compuesto por infraestructuras de tecnología de la información -incluyendo internet-, redes de telecomunicaciones y sistemas de información que configura un ámbito virtual.

– Ciberincidente: Incidente relacionado con la seguridad de las tecnologías de la información y las comunicaciones que se produce en el ciberespacio.

– Ciberseguridad (seguridad de los sistemas de información): la capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos.

– Compromiso de la seguridad: incidente de seguridad en el que, debido a una violación de las medidas técnicas u organizativas de seguridad, una información o un servicio quedan expuestos, o potencialmente expuestos, a un acceso no autorizado.

– Confidencialidad: propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

– Contraseña: un secreto memorizado por el usuario, compuesto por varios caracteres según unas reglas de complejidad frente a ataques de adivinación o fuerza bruta.

– Contraseña de un solo uso (*OTP - One-Time Password*): contraseña generada dinámicamente y que solamente se puede usar una vez y durante un periodo limitado.

– Disponibilidad: propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

– Dispositivo de autenticación (*token*): autenticador físico.

– Distintivo de Certificación de Conformidad con el ENS: documento electrónico, en formato PDF-A, firmado electrónicamente por la Entidad de Certificación responsable de la evaluación de los sistemas de información concernidos, incluyendo un enlace a la Certificación de Conformidad con el ENS que, mientras se mantenga su vigencia, permanecerá accesible a través de la sede electrónica o página web de la entidad pública o privada, respectivamente, de que se trate.

– Distintivo de Declaración de Conformidad con el ENS: documento electrónico, en formato PDF-A, firmado o sellado electrónicamente por la entidad bajo cuya responsabilidad se encuentre el sistema de información en cuestión, incluyendo un enlace a la Declaración de Conformidad con el ENS que, mientras se mantenga su vigencia, permanecerá accesible a través de la sede electrónica o página web de la entidad pública o privada de que se trate.

– Dominio de seguridad: colección de activos uniformemente protegidos, típicamente bajo una única autoridad. Los dominios de seguridad se utilizan para diferenciar entre zonas en el sistema de información. Por ejemplo:

a) Instalaciones centrales, sucursales, comerciales trabajando con portátiles.
b) Servidor central (host), frontal Unix y equipos administrativos.
c) Seguridad física, seguridad lógica.

– Evento de seguridad: ocurrencia identificada de un sistema, servicio o estado de red que indica un posible incumplimiento de la política de seguridad de la información, una falla de los controles o una situación desconocida que puede ser relevante para la seguridad.

– Factor de autenticación: hay 3 tipos de factores de autenticación: (1) algo que se sabe, un secreto; (2) algo que se tiene, un autenticador; y (3) algo que se es, biometría.

– Firma electrónica: los datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar.

– Firma electrónica avanzada: la firma electrónica que cumple los requisitos contemplados en el artículo 26 del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

– Firma electrónica cualificada: una firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica.

– Gestión de incidentes: procedimientos seguidos para detectar, analizar y limitar un incidente y responder ante éste.

– Gestión de riesgos: actividades coordinadas para dirigir y controlar a una organización con respecto a los riesgos.

– Incidente de seguridad (ciberincidente o incidente): suceso inesperado o no deseado con consecuencias en detrimento de la seguridad de las redes y sistemas de información.

– Integridad: propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.

– Lista de componentes software: documento que detalla los componentes software utilizados para construir algo, sea una aplicación o un servicio.

– Medidas de seguridad: conjunto de disposiciones encaminadas a proteger al sistema de información de los riesgos a los que estuviere sometido, con el fin de asegurar sus objetivos de seguridad. Puede tratarse de medidas de prevención, de disuasión, de protección, de detección y reacción, o de recuperación.

– Mínimo privilegio: principio que determina que el diseño de la arquitectura de seguridad de un sistema garantiza el uso de los servicios y permisos mínimos necesarios para su correcto funcionamiento.

– Monitorización continua: proceso de gestión dinámica de la seguridad basado en el seguimiento de indicadores críticos de seguridad y parcheo de las vulnerabilidades descubiertas en los componentes del sistema de información.

– Observatorio Digital: un observatorio digital, en su propósito de conocer realidades de la información que se transmite a través de medios digitales, es un conjunto de capacidades para la toma de decisiones dedicado a la detección y seguimiento de anomalías en el origen, definición o diseminación de contenidos digitales, las cuales pudieran representar indicadores de amenaza.

– Perfil de cumplimiento específico: conjunto de medidas de seguridad, comprendidas o no en el anexo II de este real decreto, que, como consecuencia del preceptivo análisis de riesgos, resulten de aplicación a una entidad o sector de actividad concreta y para una determinada categoría de seguridad, y que haya sido habilitado por el CCN.

– PIN: un secreto memorizado por el usuario, compuesto por unos pocos caracteres, siguiendo unas ciertas reglas frente a ataques de adivinación.

– Política de firma electrónica, sello electrónico y certificados: conjunto de normas de seguridad, de organización, técnicas y legales para determinar cómo se generan, verifican y gestionan firmas electrónicas y sellos electrónicos, incluyendo las características exigibles a los certificados de firma o sello electrónicos.

– Política de seguridad (Política de seguridad de la información): conjunto de directrices plasmadas en un documento, que rigen la forma en que una organización gestiona y protege la información que trata y los servicios que presta.

– Principios básicos de seguridad: fundamentos que deben regir toda acción orientada a asegurar la información y los servicios.

– Proceso: conjunto organizado de actividades que se llevan a cabo para producir un producto o prestar un servicio, que tiene un principio y fin delimitados, que implica recursos y da lugar a un resultado.

– Proceso de seguridad: método que se sigue para alcanzar los objetivos de seguridad de la organización. El proceso se diseña para identificar, medir, gestionar y mantener bajo control los riesgos a que se enfrenta el sistema en materia de seguridad.

– Proceso TIC: conjunto de actividades llevadas a cabo para la concepción, elaboración, suministro y mantenimiento de un producto o servicio TIC.

– Producto TIC: elemento o grupo de elementos de las redes o los sistemas de información.

– Requisitos mínimos de seguridad: exigencias mínimas necesarias para asegurar la información tratada y los servicios prestados.

– Secreto memorizado (factor de autenticación): algo que solamente sabe el usuario autorizado. Típicamente, se concreta en una contraseña o un PIN.

– Sistema de información: cualquiera de los elementos siguientes:

1.º Las redes de comunicaciones electrónicas que utilice la entidad del ámbito de aplicación de este real decreto sobre las que posea capacidad de gestión.

2.º Todo dispositivo o grupo de dispositivos interconectados o relacionados entre sí, en el que uno o varios de ellos realicen, mediante un programa, el tratamiento automático de datos digitales.

3.º Los datos digitales almacenados, tratados, recuperados o transmitidos mediante los elementos contemplados en los números 1.º y 2.º anteriores, incluidos los necesarios para el funcionamiento, utilización, protección y mantenimiento de dichos elementos.

– TEMPEST: término que hace referencia a las investigaciones y estudios de emanaciones comprometedoras (emisiones electromagnéticas no intencionadas, producidas por equipos eléctricos y electrónicos que, detectadas y analizadas, puedan llevar a la obtención de información) y a las medidas aplicadas a la protección contra dichas emanaciones.

– Trazabilidad: propiedad o característica consistente en que las actuaciones de una entidad (persona o proceso) pueden ser trazadas de forma indiscutible hasta dicha entidad.

– USO OFICIAL: designa información con algún tipo de restricción en su manejo por su sensibilidad y confidencialidad.

– Usuarios de la organización: personal del organismo, propio o contratado, estable o circunstancial, que acceden al sistema para desarrollar las funciones o actividades que les han sido encomendadas por la organización.

– Usuarios externos: usuarios con acceso al sistema que no entran en el conjunto de usuarios de la organización. En particular, los ciudadanos administrados.

§ 7

Orden PRE/2740/2007, de 19 de septiembre, por la que se aprueba el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información

Ministerio de la Presidencia
«BOE» núm. 230, de 25 de septiembre de 2007
Última modificación: sin modificaciones
Referencia: BOE-A-2007-16830

La utilización de las Tecnologías de la Información (TI) en amplias áreas de la actividad de la Administración, así como la creciente participación de España en proyectos de desarrollo de la sociedad de la información de carácter internacional, imponen la necesidad de garantizar un nivel de seguridad en la utilización de las TI equiparable, como mínimo, al conseguido en el tratamiento tradicional de la información en soporte papel.

Por tanto, la seguridad que las TI deben poseer, ha de abarcar la protección de la confidencialidad, la integridad y la disponibilidad de la información que manejan los sistemas de información, así como la integridad y disponibilidad de los propios sistemas.

La garantía de seguridad de las Tecnologías de la Información debe estar basada en el establecimiento de mecanismos y servicios de seguridad, adecuadamente diseñados, que impidan la realización de funciones no deseadas.

Uno de los métodos, admitido internacionalmente, para garantizar la corrección y efectividad de dichos mecanismos y servicios, consiste en la evaluación de la seguridad de las TI, realizada mediante la utilización de criterios rigurosos, con posterior certificación por el organismo legalmente establecido.

El Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información, que acompaña a esta Orden Ministerial, regula el marco de actuación, y crea los organismos necesarios, para poner estos procesos de evaluación y certificación al alcance de la industria y de la Administración; todo ello basado en el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información.

La carencia actual de un esquema análogo, puede suponer un importante obstáculo para la difusión y aceptación generalizada, tanto a nivel nacional como internacional, de los diferentes productos y sistemas de las Tecnologías de la Información desarrollados en nuestro país.

En el contexto de los programas internacionales, no se puede entender criterios de evaluación y certificación de la seguridad de las TI que no sean homologables con los de otros países participantes. Por ello, es necesario la adopción de criterios internacionales, que permitan negociar el reconocimiento mutuo de certificados, resultando esencial que el Esquema al que se refiere el presente Reglamento, se equipare a los del resto de los países de nuestro entorno.

Desde hace algunos años, en España, se ha venido sintiendo la necesidad de impulsar la creación de un esquema de esta naturaleza, habiéndose llevado a cabo diversas

iniciativas para su constitución, desde el Consejo Superior de Informática y para el Impulso de la Administración Electrónica, en colaboración con el Centro Nacional de Inteligencia. También, en la Dirección General de Armamento y Material del Ministerio de Defensa, se creó un esquema orientado a satisfacer necesidades puntuales del Ministerio de Defensa.

Asimismo, se creó un laboratorio de evaluación, el Centro de Evaluación de la Seguridad de las Tecnologías de la Información (CESTI) del Instituto Nacional de Técnica Aeroespacial (INTA). Este laboratorio fue acreditado, siguiendo este mismo Reglamento, como laboratorio de evaluación de la seguridad de las Tecnologías de la Información, por resolución 1AO/38272/2005, de 13 de octubre, del Centro Criptológico Nacional, y ha contribuido, de manera decisiva, a la creación y puesta en marcha de un esquema de funcionalidad completa.

Paralelamente, España, como país consumidor de certificados, y a través del Ministerio de Administraciones Públicas, ha estado presente en el Arreglo de Reconocimiento Mutuo de Certificados Common Criteria (CCRA), desde su creación.

En ese Ministerio, se ha sentido la necesidad de crear un único esquema nacional que abarcase todo el ámbito de la actividad de evaluación y certificación y que potenciase a España a la categoría de país productor de certificados Common Criteria.

Por todo ello, la creación de un esquema nacional va a gozar, desde el principio, de aportaciones experimentadas y se va a encajar en un foro en el que su presencia es demandada.

Por otra parte, se hace necesaria la participación de un organismo de certificación, que partiendo de un conocimiento de las Tecnologías de la Información y de las amenazas y vulnerabilidades existentes, proporcione una garantía razonable a los procesos de evaluación y certificación.

Dicho organismo se constituye al amparo de la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, que encomienda a este Centro el ejercicio de las funciones relativas a la seguridad de las Tecnologías de la Información, y según lo dispuesto en el Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional, entre cuyas funciones está la de constituir el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información.

En virtud de los preceptos indicados anteriormente, consultados los fabricantes e importadores del sector, y a propuesta conjunta de los Ministros de Defensa y de Industria, Turismo y Comercio, con la aprobación previa de la Ministra de Administraciones Públicas, dispongo:

Artículo único. *Aprobación del Reglamento.*

Se aprueba el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información, cuyo texto se inserta a continuación.

Disposición adicional única. *Naturaleza y establecimiento de la contraprestación exigida por las acreditaciones y certificaciones.*

1. Al amparo de lo dispuesto en la Ley 8/1989, de 13 de abril, de Tasas y Precios Públicos, los ingresos procedentes de las acreditaciones de laboratorios y de las certificaciones de productos, tienen la naturaleza de tasas.

2. Según lo establecido en el artículo 2.3 del Real Decreto 1287/2005, de 28 de octubre, por el que se modifica el Real Decreto 593/2002, de 28 de junio, que desarrolla el régimen económico presupuestario del Centro Nacional de Inteligencia, el establecimiento o modificación de la cuantía de los ingresos que tengan la naturaleza de tasas, así como la fijación de los diversos elementos de la correspondiente relación jurídico-tributaria, se harán con arreglo a lo dispuesto en la Ley 8/1989, de 13 de abril, de Tasas y Precios Públicos.

Disposición final primera. *Facultades de ejecución y aplicación.*

Se faculta al Secretario de Estado Director del Centro Criptológico Nacional del Centro Nacional de Inteligencia, para dictar cuantas instrucciones sean necesarias para la ejecución y aplicación de lo establecido en esta orden ministerial.

Disposición final segunda. *Entrada en vigor.*

La presente orden ministerial entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

REGLAMENTO DE EVALUACIÓN Y CERTIFICACIÓN DE LA SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

El presente Reglamento tiene por objeto la articulación del Organismo de Certificación (OC) del Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información (ENECSTI) en el ámbito de actuación del Centro Criptológico Nacional, según lo dispuesto en la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, y en el Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional, respectivamente.

Artículo 2. *Definiciones.*

En el marco del presente Reglamento, los conceptos que a continuación se indican, se entenderán como están definidos.

Acreditación.–Declaración de conformidad de los laboratorios solicitantes, emitida por el Organismo de Certificación, en base al cumplimiento de los requisitos establecidos en el Capítulo III, y según el procedimiento establecido en el Capítulo IV, del presente Reglamento.

Acreditación de competencia técnica.–Es aquella acreditación que concede una entidad de acreditación reconocida a un laboratorio, conforme a lo regulado en la Ley 21/1992, de 16 de julio, de Industria y en el Real Decreto 2200/1995, de 28 de diciembre, por el que se aprueba el Reglamento de la infraestructura para la calidad y seguridad industrial, y en base al cumplimiento, por parte del laboratorio, de la norma UNE-EN ISO/IEC 17025. En su alcance se deberán incluir las normas de evaluación de la seguridad de los productos y sistemas de Tecnologías de la Información aprobadas por el Organismo de Certificación.

Certificación.–Es la determinación, obtenida mediante un proceso metodológico de evaluación, de la conformidad de un producto con unos criterios preestablecidos.

Declaración de seguridad.–Conjunto de requisitos y especificaciones de las propiedades de seguridad de un producto o sistema de las Tecnologías de la Información.

Evaluación.–Es el análisis, realizado mediante un proceso metodológico, de la capacidad de un producto o sistema de las Tecnologías de la Información para proteger las condiciones de la información de acuerdo a unos criterios establecidos, con objeto de determinar si puede ser certificado.

Información de las evaluaciones.–Es todo asunto, acto, documento, dato u objeto relacionado con la actividad de evaluación de la seguridad de un producto. La información de las evaluaciones incluye toda la documentación, programas de ordenador, esquemas, planos y demás datos suministrados por el fabricante, los programas de ordenador, planes, pruebas, análisis y resultados de la evaluación elaborados por el laboratorio, así como toda la documentación administrativa y contractual y las comunicaciones del laboratorio con el fabricante del producto y con el Organismo de Certificación, además de los registros de la actividad del laboratorio, incluyendo los de seguridad.

Producto a evaluar.–Es el producto, sistema de información o perfil de protección para el que se solicita una certificación de sus propiedades de seguridad.

Producto clasificado.–Son aquellos productos con requisitos específicos para manejar con seguridad materias clasificadas, o cuya información de especificación, diseño o desarrollo está clasificada, incluso parcialmente, según lo dispuesto en la Ley 9/68, de 5 de abril, sobre Secretos Oficiales, modificada por la Ley 48/78, de 7 de octubre.

Laboratorio de evaluación.–Es un laboratorio de ensayo, según se define en el Real Decreto 2200/1995, de 28 de diciembre, por el que se aprueba el Reglamento de la infraestructura para la calidad y seguridad industrial.

Sistema de información.–Es el conjunto de elementos «hardware», «software», datos y usuarios que, relacionados entre sí, permiten el almacenamiento, transmisión, transformación y recuperación de la información.

Artículo 3. *Ámbito de aplicación.*

El ámbito de actuación del Organismo de Certificación comprende las entidades públicas o privadas que quieran ejercer de laboratorios de evaluación de la seguridad de las TI en el marco del Esquema.

También comprende a estas entidades cuando sean fabricantes de productos o sistemas de TI que quieran certificar la seguridad de dichos productos, en el marco del Esquema.

Todo ello, siempre que dichos productos o sistemas sean susceptibles de ser incluidos en el ámbito de actuación del Centro Criptológico Nacional.

CAPÍTULO II

Estructura y funciones del organismo de certificación

Sección 1.ª Estructura del organismo de certificación

Artículo 4. *Estructura.*

A los efectos de funcionamiento del Organismo de Certificación, su estructura será la siguiente:

a) Director del Organismo de Certificación, que será el Secretario de Estado Director del Centro Criptológico Nacional.

b) Secretario General del Organismo de Certificación, que será el Secretario General del Centro Criptológico Nacional.

c) Subdirector de Certificación, que será un funcionario del Centro Nacional de Inteligencia, con rango de Subdirector General, designado por el Director del Organismo de Certificación.

d) Jefe del Área de Certificación, que será un funcionario del Centro Criptológico Nacional, con rango de Subdirector General Adjunto, designado por el Subdirector de Certificación.

e) Los correspondientes Responsables, Técnico de Certificación, de Calidad, de Seguridad, y de Registro, que serán funcionarios del Centro Criptológico Nacional designados por el Jefe del Área de Certificación.

f) Personal técnico de certificación, que serán funcionarios del Centro Criptológico Nacional designados por el Jefe del Área de Certificación.

g) Personal de enlace con los servicios de Secretaría, y demás personal de soporte administrativo a las actividades del Organismo de Certificación, que serán funcionarios del Centro Criptológico Nacional designados por el Jefe del Área de Certificación.

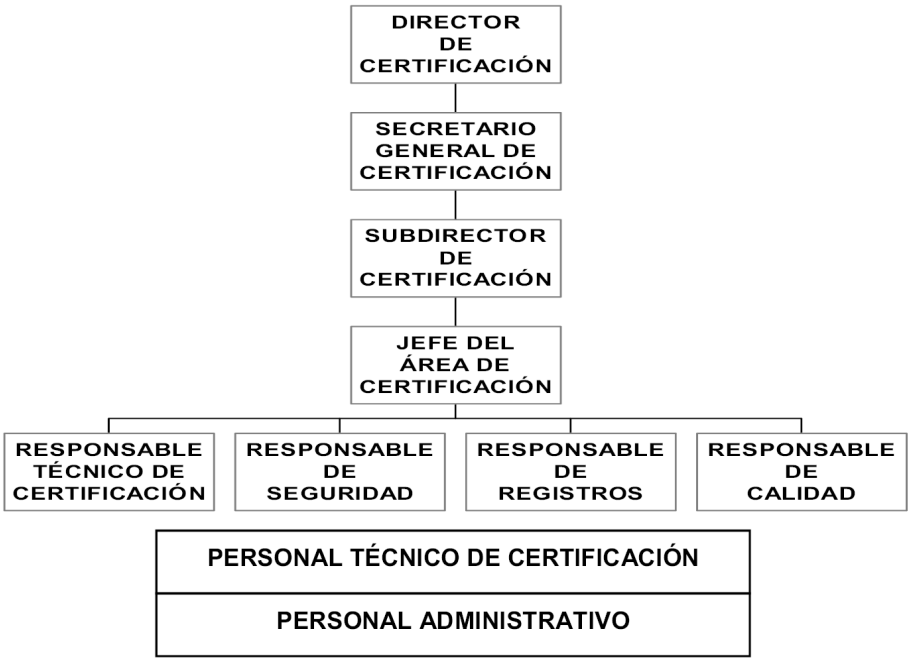


Figura 1. Estructura del Organismo de Certificación

Sección 2.ª Funciones de los cargos del organismo de certificación

Artículo 5. *Director del Organismo de Certificación.*

Corresponde al Director del Organismo de Certificación:

a) Aprobar y hacer cumplir las políticas, manuales y procedimientos que regulan la actuación del Organismo de Certificación, garantizando la adecuación de la organización y de los medios materiales y humanos a los fines propuestos.

b) Dictar las resoluciones sobre las solicitudes de acreditación de laboratorios y de certificación de la seguridad de productos y sistemas de las Tecnologías de la Información.

c) Establecer los acuerdos oportunos con otros organismos similares en el ámbito de su competencia.

Artículo 6. *Secretario General del Organismo de Certificación.*

Corresponde al Secretario General del Organismo de Certificación:

a) Apoyar y asistir al Director del Organismo de Certificación en el ejercicio de sus funciones.

b) Establecer los mecanismos y sistemas de organización del Organismo de Certificación y determinar las actuaciones precisas para su actualización y mejora.

c) Dirigir el funcionamiento de los servicios comunes del Organismo de Certificación a través de las correspondientes instrucciones y órdenes de servicio.

d) Desempeñar la jefatura superior del personal del Organismo de Certificación, elaborar la propuesta de relación de puestos de trabajo y determinar los puestos vacantes a proveer durante cada ejercicio.

Artículo 7. *Subdirector de Certificación.*

Corresponde al Subdirector de Certificación:

a) Presidir el Consejo de Acreditación y Certificación, conforme a lo establecido en el presente Reglamento.

b) Representar al Organismo de Certificación en aquellos foros de índole técnica, de normalización y de divulgación de las actividades del citado organismo, de las normas aplicables y en los de arreglos y acuerdos de reconocimiento mutuo.

c) Revisar las políticas, manuales y procedimientos que regulan la actuación del Organismo de Certificación.

d) Proponer los presupuestos y planes de formación anuales del Organismo de Certificación.

Artículo 8. *Jefe del Área de Certificación.*

Corresponde al Jefe del Área de Certificación:

a) Desempeñar la dirección de los servicios técnicos del Organismo de Certificación.

b) Dirigir las instrucciones y procedimientos de acreditación de laboratorios y de certificación de productos.

c) Elevar las correspondientes propuestas de resolución a las mencionadas solicitudes de acreditación y certificación.

d) Instruir, de oficio, los procedimientos de mantenimiento de la acreditación de los laboratorios.

Artículo 9. *Responsable Técnico de Certificación.*

Corresponde al Responsable Técnico de Certificación:

a) Apoyar y asistir al Jefe del Área de Certificación en el ejercicio de sus funciones.

b) Coordinar y dirigir la actuación diaria del personal técnico del Organismo de Certificación.

c) Realizar la asignación de personal técnico a la instrucción de cada solicitud de acreditación de laboratorio y de certificación de producto.

d) Dictaminar las interpretaciones técnicas de normas, métodos y procedimientos de evaluación empleados, bien de oficio, o a instancia de los laboratorios.

e) Elaborar o proponer las políticas, manuales y procedimientos que regulan la actuación del Organismo de Certificación.

Artículo 10. *Responsable de Calidad del Organismo de Certificación.*

Corresponde al Responsable de Calidad del Organismo de Certificación:

a) Garantizar y auditar la ejecución del sistema de gestión de la calidad del Organismo de Certificación, con las funciones específicas en él indicadas.

b) Proponer, al Jefe del Área de Certificación, las mejoras convenientes para la eficacia del sistema de gestión de calidad, tras su evaluación.

Artículo 11. *Responsable de Seguridad del Organismo de Certificación.*

Corresponde al Responsable de Seguridad del Organismo de Certificación:

a) Garantizar y auditar la ejecución del sistema de gestión de la seguridad del Organismo de Certificación, con las funciones específicas en él indicadas.

b) Proponer, al Jefe del Área de Certificación, las mejoras convenientes para la eficacia del sistema de gestión de la seguridad, tras su evaluación.

Artículo 12. *Responsable de Registro del Organismo de Certificación.*

Corresponde al Responsable de Registro del Organismo de Certificación, la gestión y custodia de los registros de calidad, seguridad, certificación y acreditación, manejados por el Organismo de Certificación.

Artículo 13. *Personal técnico del Organismo de Certificación.*

Corresponde al personal técnico del Organismo de Certificación, el desarrollo de la instrucción de los expedientes de acreditación de laboratorio y de certificación de productos,

practicando las pruebas conforme a los medios y procedimientos establecidos por el Organismo de Certificación.

Sección 3.ª Consejo de acreditación y certificación

Artículo 14. *Naturaleza.*

El Consejo de Acreditación y Certificación es un órgano colegiado, distinto e independiente del Organismo de Certificación, regido por lo establecido en el Capítulo II del Título II, de la Ley 30/92, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común y, por lo establecido en el presente Reglamento.

Artículo 15. *Composición.*

Corresponde al Subdirector de Certificación la presidencia del Consejo de Acreditación y Certificación.

Formarán parte como miembros del Consejo, los siguientes:

a) El Jefe del Área de Certificación, que podrá asumir la presidencia del Consejo por delegación del Subdirector de Certificación.

b) El Responsable Técnico de Certificación, que hará las veces de Secretario del Consejo.

c) Un representante del Ministerio de Defensa, cuyo nombramiento y asistencia solicitará el Organismo de Certificación a dicho Ministerio.

d) Un representante del Ministerio de Industria, Turismo y Comercio, cuyo nombramiento y asistencia solicitará el Organismo de Certificación a dicho Ministerio.

e) Un representante del Consejo Superior de Administración Electrónica, cuyo nombramiento y asistencia solicitará el Organismo de Certificación a dicho Consejo.

f) Un representante de cada laboratorio acreditado, nombrado por dicho laboratorio.

g) Dos representantes de los sectores empresariales de fabricantes, importadores e integradores de productos y sistemas de las Tecnologías de la Información, a propuesta razonada y acordada de dichos sectores.

Artículo 16. *Fines.*

Corresponde al Consejo de Acreditación y Certificación:

a) Vigilar que la normativa del Organismo de Certificación se corresponda y equipare con los términos y referencias de esquemas de certificación equivalentes, que pudieran existir en el ámbito de la Unión Europea en particular, y en el ámbito internacional, en general.

b) Asesorar al Organismo de Certificación en la evolución de sus procedimientos documentados, orientando la gestión de éste, al mejor servicio del tejido industrial y empresarial de fabricantes, importadores e integradores de productos y sistemas de Tecnologías de la Información.

c) Asesorar al Organismo de Certificación en la identificación de esquemas, arreglos o acuerdos, donde la defensa de la validez y reconocimiento mutuo de los certificados emitidos sea de interés para la Administración y el sector privado español.

Artículo 17. *Atribuciones.*

Las atribuciones del Consejo de Acreditación y Certificación son las siguientes:

a) Estar permanentemente informado de la normativa que regula el funcionamiento del Organismo de Certificación, incluyendo sus normas de evaluación y certificación, manuales, procedimientos e instrucciones técnicas.

b) Estar permanentemente informado de la relación de laboratorios acreditados y de productos certificados.

c) Estar permanentemente informado de la relación de esquemas de certificación de la seguridad de los productos y sistemas de información, con los que el Organismo de

Certificación tiene establecidos arreglos o acuerdos de reconocimiento mutuo de certificados.

d) Proponer directrices y recomendaciones al Organismo de Certificación, que serán recogidas en las correspondientes actas de las reuniones del Consejo, a las que deberá dar cumplida respuesta el Director del Organismo de Certificación.

Artículo 18. *Periodicidad de las reuniones.*

El Consejo de Acreditación y Certificación se reunirá, como mínimo, una vez al año, sin perjuicio de que en atención a las necesidades derivadas del cumplimiento de sus fines y atribuciones, requiera de una mayor frecuencia en las reuniones.

Las reuniones se convocarán a requerimiento del Organismo de Certificación, o por acuerdo del propio Consejo de Acreditación.

Sección 4.ª Acreditación y certificación

Artículo 19. *Acreditación de laboratorios.*

El Organismo de Certificación acredita a los laboratorios solicitantes, en base al cumplimiento de los requisitos establecidos en el Capítulo III, y según el procedimiento establecido en el Capítulo IV de este Reglamento.

Artículo 20. *Certificación de productos.*

El Organismo de Certificación certifica la seguridad de los productos y sistemas de Tecnologías de la Información, según lo establecido en el procedimiento del Capítulo V, y atendiendo a los criterios, métodos y normas de evaluación de la seguridad, establecidos en el Capítulo VI.

Artículo 21. *Publicaciones del Esquema.*

El Organismo de Certificación mantendrá actualizada la relación de laboratorios acreditados y la de productos y sistemas de las Tecnologías de la Información certificados. Dicha relación se podrá consultar en la siguiente dirección electrónica: http://www.oc.ccn.cni.es.

CAPÍTULO III

Requisitos de acreditación de laboratorios

Artículo 22. *Requisitos generales para la acreditación de laboratorios.*

1. Para la acreditación de los laboratorios de evaluación de la seguridad de las Tecnologías de la Información se requerirá el cumplimiento de los siguientes requisitos:

a) Capacidad para la evaluación de la seguridad de productos de las Tecnologías de la Información, demostrada mediante la acreditación de la competencia técnica en vigor, conforme a la norma UNE-EN ISO/IEC 17025, cuyo alcance incluya los criterios, métodos y normas de evaluación recogidos en el Capítulo VI.

b) Cumplimiento de los requisitos de seguridad establecidos en la Sección 1.ª o en la Sección 2.ª de este Capítulo, según corresponda.

c) Desarrollo de las evaluaciones de acuerdo a procedimientos que recojan las obligaciones de información y coordinación con el Organismo de Certificación, indicadas en la Sección 3.ª de este mismo Capítulo.

2. La comprobación del cumplimiento de estos requisitos se realizará mediante el procedimiento de auditoría y seguimiento indicado en las Secciones 4.ª y 5.ª del Capítulo IV.

En todo caso, el alcance de la acreditación, otorgada por el Organismo de Certificación, estará limitado por el alcance de la acreditación de la competencia técnica del laboratorio, y cualificado por el nivel de seguridad del mismo.

3. Salvo en los casos en que haya una compartimentación organizativa, de medios y de procedimientos, aprobada por el Organismo de Certificación, el laboratorio deberá cumplir

con los requisitos de gestión de seguridad, necesarios para la acreditación, incluso en el desarrollo de aquellas evaluaciones cuyo objeto final no sea la certificación del producto evaluado por parte del Organismo de Certificación.

Sección 1.ª Requisitos de seguridad para laboratorios que evalúen productos clasificados

Artículo 23. *Requisitos de laboratorios que evalúen productos clasificados.*

Los laboratorios, tanto de titularidad pública como privada, que pretendan evaluar productos clasificados deberán cumplir, además de los requisitos establecidos para los laboratorios que evalúen productos no clasificados, lo dispuesto en la Orden Ministerial Comunicada 17/2001, de 29 de enero, por la que se aprueba el Manual de Protección de Materias Clasificadas del Ministerio de Defensa en poder de las empresas.

Asimismo, deberán tener suscrito, y en vigor, Acuerdo de Seguridad, con un grado de calificación de seguridad igual o superior al grado de calificación de seguridad de la información del producto a evaluar.

Sección 2.ª Requisitos de seguridad para laboratorios que evalúen productos no clasificados

Artículo 24. *Requisitos de laboratorios que evalúen productos no clasificados.*

Los laboratorios, tanto de titularidad pública como privada, que evalúen productos no clasificados, cumplirán con los requisitos de gestión de la seguridad, aplicables a la información de las evaluaciones, establecidos en esta Sección.

Subsección 1.ª Responsabilidades del laboratorio

Artículo 25. *Derecho de acceso a la información de las evaluaciones.*

El laboratorio facilitará al Organismo de Certificación el acceso a toda la información de las evaluaciones que lleve a cabo.

El laboratorio deberá obtener, del Organismo de Certificación, autorización escrita antes de permitir a terceros, incluido el fabricante del producto evaluado, cualquier tipo de acceso a la información de las evaluaciones, tales como, planes, pruebas, análisis y resultados de la evaluación.

El Organismo de Certificación podrá prohibir la difusión de determinada información originada por el laboratorio.

Artículo 26. *Plan de protección.*

1. El laboratorio deberá elaborar, poner en práctica y mantener al día un Plan de Protección de la Información de las evaluaciones.

2. Este plan incluirá, al menos, la siguiente información:

a) Una descripción del laboratorio, con indicación expresa de la ubicación, actividades empresariales distintas a las de evaluación, en su caso, organigrama, recursos humanos, factorías, sucursales y dependencias autónomas, incluyendo un plano con leyenda de las instalaciones del laboratorio.

b) Los fundamentos del Plan, que deberán comprender los objetivos concretos que han de alcanzarse con el mismo y que estarán dirigidos a prevenir, detectar y rehabilitar el daño causado por la manifestación del riesgo, así como la identificación de los riesgos contra los que se pretende la protección.

La confidencialidad, integridad y disponibilidad de la información de las evaluaciones serán del máximo interés para el Organismo de Certificación.

c) La descripción de la organización, donde se debe documentar la estructura de seguridad del laboratorio, la matriz de responsabilidades donde se establece la identificación exacta de los responsables en lo referente a la toma de decisiones, y la definición detallada de las misiones de cada componente del sistema, así como la coordinación del apoyo

potencial de organismo exteriores, tales como empresas de seguridad privada, centrales receptoras de alarmas, servicios de custodia de información, etc.

d) La descripción de las medidas de protección física, y el establecimiento de zonas de acceso restringido en las distintas dependencias del laboratorio.

e) Los Procedimientos Operativos de seguridad.

f) La descripción de las reacciones específicas a cada incidente de seguridad, desarrollando la matriz de responsabilidades en los cometidos y misiones que este plan asigne a la dirección del laboratorio, a los que formen parte del Servicio de Protección del laboratorio y al resto de personal, en lo que respecta a decisiones y actuaciones ante los riesgos de seguridad que se manifiesten y que se hayan considerado.

g) Los requisitos específicos de seguridad y los Procedimientos Operativos de seguridad de los sistemas de información del laboratorio.

Artículo 27. *Procedimientos Operativos de seguridad.*

1. Los Procedimientos Operativos de seguridad incluirán, en forma de directivas, los detalles específicos de actuación encaminados a la prevención de riesgos.

2. Estas actuaciones se deben corresponder con la matriz de responsabilidades, tratando de forma concreta y específica los siguientes aspectos, relativos a requisitos de seguridad establecidos por las condiciones de acreditación del laboratorio:

a) Las normas para el manejo y custodia de la información de las evaluaciones.

b) El tratamiento de las visitas, verificando periódicamente la eficacia del control de visitas al laboratorio, así como el correcto uso del libro de visitas o sistema alternativo.

c) La entrada en las zonas de acceso restringido.

d) El acceso, transmisión, reproducción, archivo y destrucción de información de las evaluaciones, con el establecimiento de los mecanismos necesarios que permitan identificar, en todo momento, al responsable de la tenencia de la información.

e) La regulación de las necesarias comprobaciones de seguridad, tanto durante la jornada de trabajo como al término de la misma.

f) La descripción del sistema de control de llaves.

g) El establecimiento del sistema de recibo interno, para control de información de las evaluaciones.

h) La operativa de actuación ante una incidencia de la central receptora de alarmas.

i) Los procedimientos de actuación de los vigilantes de seguridad.

Artículo 28. *Personal del laboratorio.*

El laboratorio deberá mantener actualizado un registro de seguridad de todo el personal afecto al mismo.

El laboratorio regulará, en base a la necesidad de conocer, el acceso de dicho personal a la información de las evaluaciones. Las autorizaciones de acceso a la información de las evaluaciones se comunicarán y revocarán por escrito, adjuntándose dichas comunicaciones al registro de seguridad del personal.

Artículo 29. *Comunicaciones preceptivas al Organismo de Certificación.*

El laboratorio deberá informar al Organismo de Certificación, en el plazo más breve posible, de lo siguiente:

a) Sobre toda información que llegue a su conocimiento en relación con accesos, o intentos de acceso, no autorizados a información de las evaluaciones; actos de sabotaje, o actividades que supongan un riesgo para dicha información.

b) Sobre toda anomalía, extravío, robo o manipulación relacionada con la información de las evaluaciones.

c) Sobre la presunción de que una transmisión de información de las evaluaciones haya sufrido vulneración o retraso injustificado.

d) Sobre las modificaciones que pretenda realizar en las zonas de acceso restringido.

e) Sobre las visitas que reciba conforme a lo que se expresa en la Subsección 5.ª, presente Capítulo y Sección.

f) Sobre las modificaciones del Plan de Protección, así como de las altas y bajas de personal y sobre la composición y cambios del Servicio de Protección.

Artículo 30. *Relaciones del laboratorio con contratistas.*

Los requisitos de seguridad requeridos por la acreditación del laboratorio, son también de aplicación a los contratistas del mismo que vayan a acceder a información de las evaluaciones.

El laboratorio deberá obtener, del Organismo de Certificación, autorización escrita antes de proporcionar al contratista el acceso a información de las evaluaciones. En su solicitud, comunicará los datos de identificación del contratista, así como la información de las evaluaciones a las que pudiera tener acceso, y el objeto y condiciones específicas de dicho acceso.

Como norma general, para la concesión de la autorización de acceso, el contratista deberá demostrar el cumplimiento de los requisitos de seguridad establecidos en el presente Reglamento mediante auditoría del Organismo de Certificación, conforme al procedimiento establecido en el Capítulo IV, salvo en los casos en que el Organismo de Certificación determine la aplicación de condiciones o limitaciones particulares a dicho acceso.

Subsección 2.ª Tratamiento de la información de las evaluaciones

Artículo 31. *Distintivos.*

1. Toda información de las evaluaciones llevará, de forma clara y visible, un signo distintivo de tal condición, que indicará la evaluación a la que corresponde.

2. Si se trata de documentos sueltos, se pondrá el signo distintivo en la parte superior e inferior de cada una de las páginas, centrado en las mismas, de tal forma que no pueda quedar oculto por dobleces, grapas, cubiertas, etc.

3. Si se trata de documentos permanentemente unidos o encuadernados, se pondrá el mencionado distintivo en la cubierta anterior y posterior, así como en todas sus páginas, conforme a lo indicado anteriormente.

4. Si se trata de planos, diagramas, esquemas o documentos similares, dicho distintivo se situará en la carátula y en la parte que identifique el documento.

5. Los soportes y sistemas informáticos que contengan o procesen información de las evaluaciones, se marcarán con los distintivos apropiados, para lo cual podrán emplearse etiquetas o cintas adhesivas.

6. Se seguirán procedimientos análogos para la protección de la información de las evaluaciones soportada en cualquier elemento, o conjunto de elementos, físicamente separables.

Artículo 32. *Libro registro de información de las evaluaciones.*

1. En cada dependencia del laboratorio donde se custodie información de las evaluaciones, existirá un registro donde figurará toda la información de las evaluaciones que haya tenido entrada o salida, las reproducciones y destrucciones, así como el acceso a dicha información por personal, tanto propio, como ajeno al laboratorio, con independencia de si esta información se almacena o transmite en papel o en soporte electrónico.

2. El registro se podrá mantener en soporte informático, en soporte papel (en forma de libro) o en una combinación de ambos soportes.

3. Estos registros deberán ser custodiados con la debida protección electrónica, si están en soporte informático, o en los muebles de seguridad ubicados en la zona de acceso restringido, si están en soporte papel.

4. El laboratorio deberá implementar los mecanismos correspondientes para que el registro de entrada/salida mediante soporte electrónico no se pueda eludir por el personal del mismo.

Artículo 33. *Recepción y recibo de la información de las evaluaciones.*

Cuando se reciba cualquier información de las evaluaciones, se seguirá el siguiente proceso:

a) Se examinará el envío para asegurarse de que no ha sido violado, comprobándose el contenido contra recibo. La evidencia de violación y las anomalías que se observen en el contenido deberán notificarse, cuanto antes, al remitente y al Organismo de Certificación.

b) Cuando el envío esté en orden, se firmará el recibo y se devolverá debidamente cumplimentado al remitente, realizando de manera inmediata la anotación en el libro registro.

Artículo 34. *Transmisión de la información de las evaluaciones.*

1. Se entiende por transmisión de la información de las evaluaciones, su traslado, comunicación, envío, entrega o divulgación a terceros.

2. Será necesario que la transmisión y custodia de la información de las evaluaciones sea controlada por un sistema de recibos, incluso dentro de las dependencias del laboratorio, con el fin de identificar, en cualquier momento, al responsable de su tenencia.

3. Cuando se trate de transmisión no electrónica de información de las evaluaciones, se realizará de la siguiente forma:

a) Por entrega directa del personal del laboratorio.

b) Por correo certificado nacional.

c) Por transportistas comerciales.

d) El embalaje de la información se llevará a cabo de forma que se pueda detectar su apertura; con cubiertas opacas que impidan desvelar su contenido, de tal naturaleza y resistencia, que aseguren su integridad durante el transporte; y, dicho embalaje, no tendrá ninguna indicación externa de la información contenida.

4. Cuando se trate de transmisión electrónica de información de las evaluaciones, se realizará utilizando las medidas técnicas y operacionales de protección de su confidencialidad que determine, en cada caso, el Organismo de Certificación.

Artículo 35. *Reproducción de la información de las evaluaciones.*

1. El número de reproducciones de la información de las evaluaciones, será el mínimo imprescindible. Se controlará mediante una correlativa numeración, que se recogerá en el registro, como anotación suplementaria del correspondiente original, indicando todos los datos referentes a dichas reproducciones y a la situación de cada una de ellas.

2. Cada reproducción, total o parcial, de información de las evaluaciones deberá ser numerada y tratada, a todos los efectos, como el original.

3. La reproducción de información de las evaluaciones deberá realizarse directamente por el laboratorio, sin recurrir a contratistas de artes gráficas. Se deberá comprobar, después de realizar las reproducciones, que en el mecanismo de reproducción no queda registro de la información reproducida.

Artículo 36. *Custodia y destrucción de la información de las evaluaciones.*

1. El laboratorio custodiará, por un plazo mínimo de cinco años, toda la información de cada evaluación, a contar desde la fecha de emisión del certificado correspondiente, o de la emisión del último informe técnico de evaluación, en el caso de productos no certificados.

2. En el caso de reevaluaciones, mantenimiento o extensiones del certificado, el cómputo de cinco años se referirá siempre al último certificado o informe técnico de evaluación aplicable.

3. Pasado dicho plazo, y tras obtener del Organismo de Certificación autorización escrita, procederá a su destrucción, de forma que se garantice que la información de las evaluaciones queda irreconocible y se impida su reconstrucción, total o parcial.

4. El Organismo de Certificación, previo a la autorización de destrucción, podrá requerir al laboratorio el traslado de cuanta información de las evaluaciones sea de su interés.

Artículo 37. *Inventario anual.*

El laboratorio presentará ante el Organismo de Certificación, antes del diez de enero de cada año, un inventario anual de toda la información de las evaluaciones que obran en su poder a fecha treinta y uno de diciembre del año anterior.

Subsección 3.ª Servicio de Protección de la información de las evaluaciones

Artículo 38. *Miembros del Servicio de Protección.*

1. En la organización del laboratorio, el Servicio de Protección de la información de las evaluaciones estará constituido, al menos, por el jefe del Servicio de Protección, el director del Servicio de Protección y el administrador de seguridad del sistema de información.

2. Los miembros del Servicio de Protección nombrados en el párrafo anterior son los responsables, ante el Organismo de Certificación, de la correcta aplicación de los requisitos de seguridad indicados, por ello deben contar con el adecuado grado de representatividad y autoridad, dentro de la organización del laboratorio.

3. Sus funciones de seguridad no podrán quedar disminuidas en ningún momento, aún cuando desempeñen otros cometidos en el laboratorio, debiendo contar con los medios necesarios para realizar sus funciones con eficacia.

Artículo 39. *Condiciones personales y nombramiento.*

1. Los responsables del Servicio de Protección deberán tener dependencia directa de la dirección del laboratorio, una relación laboral estable sobre la base de continuidad en su función y se les reconocerá, dentro del laboratorio, la debida autoridad en el desempeño de sus cometidos.

Deberán gozar de prestigio personal y profesional, y tener un amplio conocimiento de la organización del laboratorio.

2. El nombramiento y cese de los responsables del Servicio de Protección se comunicará por escrito, reconocido expresamente, en el que constarán las misiones de la responsabilidad asignada.

3. La inadecuación en el desarrollo, o la inobservancia, de las misiones encomendadas a los responsables del Servicio de Protección, podrá motivar su cese, cuando el Organismo de Certificación así lo demande, previa notificación por escrito, y sin perjuicio de la exigencia de otras responsabilidades que se pudieran derivar.

Artículo 40. *Director del Servicio de Protección.*

1. Cuando el laboratorio designe varios jefes del Servicio de Protección de la información de las evaluaciones, uno por cada una de las sedes donde se maneje o custodie información de las evaluaciones, deberá nombrar un director del Servicio de Protección, cuya misión principal será coordinar la actuación de dichos jefes, así como de los distintos administradores de seguridad del sistema de información, sin que esto suponga merma alguna de las responsabilidades que a éstos corresponde.

2. El cargo de director del Servicio de Protección se podrá compatibilizar con el de jefe de dicho Servicio, en las dependencias donde se ubiquen las oficinas centrales del laboratorio.

Artículo 41. *Misiones del jefe del Servicio de Protección.*

1. Corresponde al jefe del Servicio de Protección la misión de organizar, dirigir y controlar el sistema de protección para salvaguarda de la información de las evaluaciones, y la obligación de cumplir y hacer cumplir, en todas sus partes, estos requisitos de seguridad para la acreditación del laboratorio.

2. Entre los cometidos del jefe del Servicio de Protección se encuentran:

a) Asegurar la protección de la información de las evaluaciones en poder del laboratorio.

b) Regular el acceso a la información de las evaluaciones conforme a los criterios y procedimientos establecidos.

c) Llevar a cabo un programa de formación del personal del laboratorio, con una periodicidad mínima de treinta (30) meses, cuyo principal objetivo será sensibilizar a dicho personal sobre la importancia de cumplir los procedimientos de protección de la información de las evaluaciones y el deber de discreción.

d) Controlar la recepción, custodia, reproducción, destrucción y devolución de la información de las evaluaciones, conforme a los procedimientos establecidos.

e) Velar, especialmente, para que ninguna información de las evaluaciones sea transmitida indebidamente, o sea manejada o custodiada en lugar distinto a las zonas protegidas.

f) Elaborar, implantar y mantener el Plan de Protección conforme a lo establecido en este Reglamento.

g) Mantener actualizados los registros de seguridad.

Artículo 42. *Misión del administrador de seguridad del sistema de información.*

1. El administrador de seguridad del sistema de información tendrá como misión organizar, dirigir y controlar la seguridad del sistema de información del laboratorio. Este administrador podrá ser el propio jefe del Servicio de Protección, cuando tenga la formación adecuada.

2. Entre los cometidos del administrador de seguridad del sistema de información se encuentran:

a) Elaborar, organizar e implementar los requisitos y procedimientos relativos a la seguridad de los sistemas de información del laboratorio, debiendo revisar, periódicamente, la eficacia de todos los componentes.

b) Controlar que todo el personal que tiene acceso al sistema de información está debidamente autorizado.

c) Investigar los incidentes de seguridad que pudieran afectar al sistema de información, evaluando en su caso, los daños causados e informando de las conclusiones al jefe del Servicio de Protección.

d) Llevar a cabo un programa de formación continua de los usuarios del sistema de información, sobre la observancia de los procedimientos de seguridad.

e) Gestionar y proporcionar los códigos de acceso u otros dispositivos de control de acceso al sistema de información. Llevará un registro de asignación de códigos a los usuarios, que serán cambiados con una periodicidad mínima de tres meses, y cada vez que se produzca, o se sospeche que haya ocurrido, un incidente de seguridad que comprometa dichos códigos.

f) Realizar la gestión de claves del sistema de información del laboratorio, incluidos los sistemas de cifra que estuvieran en el ámbito de su competencia, así como la de los sistemas de soporte a la evaluación. Para ello, controlará su generación, almacenamiento, distribución, expiración y destrucción. En la recepción de nuevos equipos modificará todas las claves que, por defecto, vengan de fábrica.

g) Controlar tanto las modificaciones que se realicen en cualquier componente del sistema de información, asegurándose que no se vea afectada la seguridad del sistema, como los aspectos de la gestión de la configuración de dichas modificaciones.

h) Comprobar que el mantenimiento del sistema de información se realiza conforme a los procedimientos y requisitos operativos de seguridad.

i) Verificar que los soportes de almacenamiento que incluyan información de las evaluaciones se custodian debidamente.

j) Evaluar los registros de seguridad del sistema de información, asegurándose que son suficientes para llevar a cabo un control eficaz. Deberán incluir aquellas actividades, con indicación del usuario, hora y fecha, en que se produzcan hechos que puedan afectar a la seguridad del sistema, como finalizaciones anormales del trabajo, cierres indebidos del sistema, fallos en los mecanismos de seguridad, intentos no autorizados de acceso a datos de la evaluación, uso del sistema de un modo no autorizado, copias e impresiones de la información de las evaluaciones, etc.

k) Controlar y registrar las copias periódicas de seguridad.

Subsección 4.ª Inspecciones de seguridad

Artículo 43. *Inspectores de seguridad.*

Los inspectores de seguridad son los representantes del Organismo de Certificación, ante el laboratorio, para la comprobación de la correcta aplicación de los requisitos de seguridad exigidos en el proceso de acreditación.

El laboratorio les reconocerá las competencias que les atribuyen estos requisitos, asumiendo el compromiso de facilitarles su labor, y dispondrá los medios precisos para que realicen sus funciones con eficacia.

Artículo 44. *Nombramiento.*

El Organismo de Certificación notificará al laboratorio la identidad del inspector de seguridad correspondiente, así como los cambios que se produzcan.

El nombramiento de inspector de seguridad, para un mismo laboratorio, podrá recaer en varias personas, si el Organismo de Certificación así lo estima oportuno.

Artículo 45. *Misiones del inspector de seguridad.*

Corresponde al inspector de seguridad:

a) La observancia del exacto cumplimiento de las obligaciones y compromisos que contrae el laboratorio en el proceso de acreditación.

b) Asesorar al laboratorio en la puesta en práctica de los procedimientos de seguridad, que garanticen la protección de la información de las evaluaciones.

Artículo 46. *Inspecciones.*

1. La inspección constituye uno de los medios por los que el Organismo de Certificación comprueba el cumplimiento, por parte del laboratorio, de los requisitos de seguridad para la acreditación.

2. Las inspecciones serán ordinarias cuando se realizan de forma periódica, por los inspectores de seguridad nombrados específicamente para cada laboratorio. Las inspecciones ordinarias no precisan concertación previa.

3. Las inspecciones extraordinarias se realizarán cuando el Organismo de Certificación lo estime conveniente, y serán llevadas a cabo por las personas que éste designe. Las inspecciones extraordinarias se comunicarán previamente al laboratorio.

4. En las inspecciones estarán obligados a estar presentes, el jefe del Servicio de Protección, o quien le sustituya, debidamente acreditado en el caso justificado de que el primero no pudiera asistir, y el personal dependiente del laboratorio que designe el Organismo de Certificación.

5. El inspector de seguridad, en las inspecciones ordinarias, o el jefe de la comisión del Organismo de Certificación, en las inspecciones extraordinarias, deberá anotar en el registro del laboratorio, un resumen del resultado de la inspección. En el caso de presentar aspectos negativos, se remitirá al laboratorio la correspondiente comunicación, en la que se deberá reflejar el plazo de corrección para solventar las anomalías observadas por la inspección.

Subsección 5.ª Visitas

Artículo 47. *Consideración de visita.*

Se considera visita, el acceso físico y circunstancial de una o varias personas, sin relación de dependencia directa con el laboratorio, a las dependencias o instalaciones del mismo.

Artículo 48. *Registro de visitas.*

Las visitas se anotarán en el registro de visitas, antes de efectuar la visita. Se deberán recoger, como mínimo, los siguientes datos: fecha de la visita, nombre completo del visitante, número del DNI o pasaporte, nacionalidad, empresa/organismo o dirección del visitante, y nombre de la persona visitada.

Este registro estará a disposición del Organismo de Certificación, para su consulta.

Artículo 49. *Normas para el control de visitas.*

Para el control de las visitas, se seguirán las siguiente normas:

a) El laboratorio controlará el movimiento de las visitas que entren en sus dependencias, para garantizar la debida seguridad de la información de las evaluaciones que custodie.

b) Se prohibirá al visitante efectuar cualquier tipo de registro o reproducción de la información de las evaluaciones, que deberá solicitarse al personal del laboratorio y ser efectuado mediante los procedimientos correspondientes.

c) Toda entrega al visitante de información de las evaluaciones será anotada en el registro.

Artículo 50. *Visitas de larga duración.*

Tendrán consideración de visitas de larga duración, las realizadas sobre la base de continuidad o reiteración, por un periodo de doce meses. Tales visitas se anotarán en el registro de seguridad de personal, incluyendo las autorizaciones de acceso a la información de evaluaciones que se pudieran conceder.

Subsección 6.ª Zonas de acceso restringido

Artículo 51. *Sistema de protección.*

1. El laboratorio implantará un sistema de protección, integrado en la estructura empresarial, que permita proteger la información de las evaluaciones contra los riesgos que puedan implicar una amenaza para la misma.

2. El sistema de protección puede entenderse como el conjunto de recursos y procedimientos que, interactuando coordinadamente, tienen como finalidad proteger la información de las evaluaciones de los riesgos que puedan afectar a su integridad, confidencialidad o disponibilidad.

Artículo 52. *Características del sistema de protección.*

El documento donde se definen las características que presenta el sistema de protección es el Plan de Protección, definido en el Artículo 26.

El laboratorio deberá adjuntar, al Plan de Protección, un proyecto del subsistema de protección física, que estará compuesto por una memoria justificativa de los criterios de diseño, la descripción detallada de todos los componentes de la instalación y los planos que especifiquen la ubicación física de los mencionados componentes.

Artículo 53. *Subsistema de protección física.*

El subsistema de protección física, que ha de instalarse, obligatoriamente, en las dependencias del laboratorio donde se vaya a manejar información de las evaluaciones, ha de mantenerse en un óptimo grado de eficacia y utilidad para el cumplimiento de las condiciones de acreditación del laboratorio. La valoración de dicha eficacia y utilidad corresponde al Organismo de Certificación.

Las áreas de acceso restringido, que deberá considerar el subsistema de protección física, están compuestas por las zonas de evaluación y las zonas de protección.

Artículo 54. *Zonas de evaluación.*

Las zonas de evaluación son las constituidas por aquellas dependencias del laboratorio en las que, únicamente, se debe manejar y custodiar información de las evaluaciones, con las siguientes características:

a) Ha de estar construida de forma que quede limitado, materialmente, el acceso a la misma, y de manera que se pueda apreciar, con una simple inspección, una intrusión a través de las paredes, suelo, puertas o ventanas que delimiten la zona. Estos elementos no deben permitir la observación desde el exterior.

b) Las puertas de acceso deben disponer de una cerradura de bloque con llave, cuyo mecanismo será obligatoriamente accionado, cuando en el interior se esté trabajando con información de las evaluaciones, así como cuando no haya nadie en la misma. También dispondrán de un dispositivo que obligue a la puerta a permanecer cerrada, cuando no se esté franqueando, y dispondrán de detector de apertura.

c) Si se incluyen ventanas, deben colocarse dispositivos que detecten su apertura, en el caso de ser practicables, así como detectores de rotura de cristales. Los elementos translúcidos deberán estar acondicionados para impedir la observación desde el exterior. En el caso de que las ventanas tengan fácil acceso desde el exterior, estarán físicamente protegidas.

d) Se implantarán medidas físicas y organizativas para impedir el acceso a la zona de evaluación, al personal que no tenga derecho de acceso a la información de las evaluaciones y, en el caso en que se divida esta zona por evaluaciones, al personal que no tenga derecho de acceso, en particular, a la información de la evaluación asociada a cada división.

e) Deberá contar con una caja fuerte Nivel IV, conforme a la norma UNE-EN 1143-1-98, equipada con cerradura Clase B, según norma EN 1300, donde se custodiará, obligatoriamente, la información de las evaluaciones durante los períodos de tiempo en que no se esté manejando. Deberá reunir, además, las características siguientes:

Si se trata de caja fuerte autónoma, ha de estar anclada si su volumen es inferior a 500 litros, o si su peso no supera los 1.000 Kg.

Si se trata de caja fuerte empotrada, el grado de seguridad del alojamiento donde se ubique ésta ha de proporcionar, como mínimo, el atribuido al de la puerta y marco de la caja.

Doble sistema de apertura, uno de los cuales ha de ser, ineludiblemente, de combinación electrónica.

Artículo 55. *Zonas de protección.*

Las zonas de protección son las constituidas por el entorno de las zonas de evaluación en el que no se podrá manejar o custodiar información de las evaluaciones, pero que estarán dotadas de medidas de seguridad, con la finalidad de incrementar la seguridad de las zonas de evaluación y tendrán las siguientes características:

a) Su ubicación dependerá de las características constructivas y de la situación de la zona de evaluación.

b) En cualquier caso, se implementarán las medidas físicas y organizativas suficientes para que el personal que acceda a la zona de protección esté identificado.

Artículo 56. *Central de alarmas.*

Además de los requisitos establecidos en los artículos 54 y 55, las zonas de evaluación y de protección dispondrán de las siguientes medidas de seguridad:

a) Todos los medios activos de seguridad deben estar conectados físicamente a un centro de control de alarmas, que disponga de una autonomía mínima de setenta y dos horas, provista de un dispositivo antisabotaje y ubicada de manera oculta.

b) Este centro de control quedará activado, obligatoriamente, fuera del horario laboral y estará conectado con una central receptora de alarmas, que pueda gestionar cualquier alarma de forma oportuna.

c) La conexión con la central receptora de alarmas debe permitir la verificación automática de la línea de comunicación, para poder conocer oportunamente una interrupción en la misma, a través de la correspondiente señal de alarma. La operativa de la gestión de la central receptora de alarmas deberá estar incluida en el Plan de Protección.

d) Los códigos de acceso de la central de alarmas, que permiten su programación y control, deberán ser conocidos, únicamente, por el jefe del Servicio de Protección y las personas por él designadas. Dicha designación quedará anotada en el registro de seguridad del personal. Los códigos deberán modificarse con los criterios indicados en el artículo 57, referido a «Combinaciones, códigos de acceso y control de llaves», que sigue.

Subsección 7.ª Procedimiento de seguridad

Artículo 57. *Combinaciones, códigos de acceso y control de llaves.*

1. Sólo tendrán conocimiento de los códigos de acceso a las zonas de evaluación, de las claves de control de la central de alarmas, así como de las combinaciones de los lugares de

custodia de la información de las evaluaciones, el jefe del Servicio de Protección y las personas que él designe, que serán las mínimas imprescindibles.

2. Las llaves de las cajas fuertes no podrán salir de la sede del laboratorio bajo ningún concepto, debiendo guardarse de forma oculta y segura, y en distinto lugar al que se custodien las claves de combinación para la apertura de las mismas.

3. Deberá ocultarse la identificación del fabricante, modelo, año de construcción u otros datos que puedan facilitar un conocimiento de las características de las cajas fuertes a las que se refieren.

4. Las claves de combinación para la apertura de las cajas fuertes y los códigos de control de la central de alarmas no deben conservarse en claro, sino de manera cifrada, debiendo ser modificados, obligatoriamente, en los siguientes casos:

a) Al recibirse los muebles de seguridad e instalarse la central de alarmas, modificando las claves y códigos que traen de fábrica.

b) Cada seis meses.

c) Cuando se produzca un cambio en las personas que hayan tenido acceso a las mismas, incluido el personal de las empresas de mantenimiento.

d) Cada vez que se produzca, o se sospeche que haya ocurrido, un incidente de seguridad que comprometa las claves o los códigos.

Artículo 58. *Acceso físico a la información de las evaluaciones.*

Cuando se precise el acceso físico a la información de las evaluaciones, el jefe del Servicio de Protección de la información, o persona designada por él, pondrá dicha información a disposición de los empleados del laboratorio que cuenten con las debidas autorizaciones de acceso a la misma, la cual deberá ser manejada exclusivamente en la zona de evaluación, estando bajo la responsabilidad de estas personas su custodia y control.

Una vez finalizado el manejo, se devolverá inmediatamente a la persona que hizo entrega de la misma, siendo almacenada en su lugar de custodia, donde permanecerá obligatoriamente.

Artículo 59. *Dispositivos técnicos de identificación.*

Siempre que el laboratorio lo considere necesario, podrá emplear dispositivos personales que faciliten y controlen el acceso, por su personal, a las zonas de acceso restringido. Los dispositivos serán diseñados de forma que se impida su empleo no autorizado, por lo que, cada uno de ellos se asignará a un empleado determinado, con su correspondiente código personalizado, que será conocido únicamente por el interesado.

De estos dispositivos no podrán determinarse las evaluaciones a cuya información tiene acceso el empleado al que se le asigna.

En su caso, deberá notificarse al Organismo de Certificación el sistema adoptado, debiéndose plasmar la operativa del mismo en el Plan de Protección.

Subsección 8.ª Seguridad de los sistemas de información

Artículo 60. *Seguridad de la información sobre evaluaciones.*

1. La información de las evaluaciones es un bien que debe ser protegido de manera que se garantice su confidencialidad, su integridad y disponibilidad, a lo largo de toda su existencia, con independencia del medio, soporte o formato en el que permanezca o se transmita. Para ello, también es necesario asegurar la integridad y disponibilidad de los servicios y recursos que sustentan dicha información.

2. Los mecanismos de seguridad del sistema de información que procese, almacene o transmita información de las evaluaciones, tienen como finalidad evitar accesos, destrucciones y modificaciones no permitidas, asegurando, al mismo tiempo, que la información es utilizada cuándo y cómo lo requieran los usuarios autorizados.

3. Los factores que se han de evaluar en la protección de la información de las evaluaciones serán los siguientes:

a) Confidencialidad, como servicio de seguridad que pretende que una información sea revelada exclusivamente a los usuarios, entidades o procesos autorizados.

b) Integridad, como medida que asegura que la información sea creada, modificada o borrada sólo por personas, entidades o procesos autorizados.

c) Disponibilidad, para que la información sea utilizable en el lugar, momento y forma que lo requieran lo usuarios, entidades o procesos autorizados.

4. El laboratorio deberá concretar los principios y reglas básicas de seguridad, exigidos para la acreditación, en unos procedimientos específicos para la protección de la información de las evaluaciones tratadas en su sistema de información, cuya seguridad deberá estar necesariamente integrada en el sistema de protección del laboratorio.

5. La seguridad del sistema de información requiere la adecuada aplicación de procedimientos y normas que posibiliten el control de acceso al sistema, la distribución de responsabilidades, la segregación de funciones y la compartimentación de los entornos correspondientes a las evaluaciones y a la administración y gestión del laboratorio.

Artículo 61. *Usuario del sistema de información.*

1. El usuario del sistema de información que maneje información de las evaluaciones dependerá directamente, en todo lo referente a la seguridad del sistema, del administrador de seguridad del sistema de información, al que informará inmediatamente del menor indicio o conocimiento de cualquier hecho que afecte a la seguridad de la información de las evaluaciones.

2. La responsabilidad de cada usuario es básica para la seguridad del sistema. Por ello es imprescindible la autenticación del usuario. Se entenderá por autenticación el proceso que confirma su identidad.

Bajo ningún concepto este usuario podrá emplear equipos y medios particulares para el tratamiento de la información de las evaluaciones.

El usuario se asegurará que su código personal no es utilizado por otra persona, recomendándose la memorización del mismo, sin dejar constancia escrita o, en su caso, guardando el registro de forma oculta y segura; no hacer uso del código cuando se está siendo observado y no compartir, en ningún caso, el código personal con otros usuarios del sistema.

3. En los sistemas que lo permitan, el usuario realizará copias periódicas de seguridad de la información de las evaluaciones, bajo la supervisión del administrador de seguridad del sistema de información, quien llevará el control y registro oportuno.

Artículo 62. *Soportes de almacenamiento de información de las evaluaciones.*

1. Los soportes removibles reutilizables, que hayan contenido información de las evaluaciones, podrán volverse a emplear una vez que se haya efectuado el borrado seguro mediante procedimientos que garanticen el mismo.

Esto también se aplicará a los soportes fijos de los equipos utilizados en las pruebas de evaluación, así como en los destinados a la instalación, o recreación, del producto a evaluar y a su entorno de pruebas, que deberán borrarse de manera segura al término de cada evaluación.

El resto de soportes fijos de información del laboratorio deberán ser tratados según procedimientos específicos, que serán reseñados en los Procedimientos Operativos de seguridad, de forma que se imposibilite la extracción de información por personal no autorizado.

2. Toda información que tenga entrada mediante comunicaciones electrónicas, o soporte removible, deberá ser comprobada en un sistema aislado, previamente a su inclusión en el sistema de información del laboratorio, a fin de detectar la posible presencia de elementos extraños, dañinos o de mal funcionamiento. Dicha comprobación, y su resultado, quedarán anotados en el libro registro del laboratorio junto con la anotación de la entrada de la información.

Artículo 63. *Características físicas de las instalaciones.*

1. El sistema de información que se utilice para el tratamiento de la información de las evaluaciones deberá estar situado en la zona de evaluación y, obligatoriamente, ubicado en territorio nacional.

2. Los equipos periféricos de impresión de documentos estarán insonorizados, cuando las características de los mismos lo requieran, y así lo determine el Organismo de Certificación.

3. No se podrá realizar ningún cambio en la ubicación física de los elementos del sistema de información, sin el control del administrador de seguridad, y la aprobación del jefe del Servicio de Protección de la información de las evaluaciones.

Artículo 64. *Procedimientos operativos de seguridad.*

1. El administrador de seguridad del sistema de información del laboratorio elaborará unos Procedimientos Operativos de seguridad, donde se describirán, detalladamente, las operaciones necesarias para proteger dicho sistema.

2. Estos procedimientos operativos de seguridad han de cumplir los requisitos de seguridad para la acreditación del laboratorio, incluirse en el Plan de Protección y, adicionalmente, contemplarán lo siguiente:

a) La revisión bianual del grado de cumplimiento de la eficacia de los propios procedimientos operativos, y del cumplimiento de los requisitos de seguridad para la acreditación del laboratorio.

b) La aplicación de medidas de protección contra elementos dañinos o maliciosos (virus, caballos de Troya, gusanos, etc.).

c) El cambio trimestral de los códigos de acceso de los usuarios.

d) La aplicación de un sistema de borrado rápido o destrucción de la información de las evaluaciones, para casos de emergencia.

e) La utilización de un sistema de alimentación ininterrumpida, de duración suficiente, para salvaguardar los procesos en curso.

Artículo 65. *Interconexión de sistemas.*

1. Como norma general, el sistema de información donde se trate información de las evaluaciones, deberá estar aislado.

Excepcionalmente pueden existir situaciones en las que el sistema necesite estar interconectado con otros, bien para comunicar varias zonas de evaluación del laboratorio, separadas físicamente, en las que se realice la misma evaluación, o para permitir la comunicación en situaciones de naturaleza análoga.

En estas situaciones, la interconexión deberá ser autorizada por el Organismo de Certificación, que determinará los requisitos de seguridad que se deben implantar.

2. El acceso del laboratorio a redes públicas, para la consulta y descarga de información de vulnerabilidades, programas de uso en las evaluaciones y demás información relevante a las evaluaciones, no se podrá realizar en las áreas de evaluación o de protección, debiendo tramitarse la incorporación de esta información al sistema de información del laboratorio, conforme a lo requerido en el artículo 32, «Libro registro de información de las evaluaciones».

Sección 3.ª Requisitos de los procedimientos de evaluación

Artículo 66. *Reconocimiento de actuaciones del laboratorio de evaluación.*

La certificación de la seguridad de un producto se inicia a instancias del solicitante ante el Organismo de Certificación, lo cual no obsta para que, independientemente, se puedan solicitar, por parte del mismo interesado, trabajos de evaluación equivalentes a los que requiere el Organismo de Certificación para la certificación de dicho producto.

En cualquier caso, el Organismo de Certificación únicamente reconocerá las actuaciones del laboratorio de evaluación que se realicen, completamente, bajo su conocimiento y

seguimiento, conforme al procedimiento establecido en el Capítulo V del presente Reglamento.

Artículo 67. *Procedimientos de evaluación.*

Los procedimientos de evaluación del laboratorio que solicite la acreditación, deberán contemplar las obligaciones de coordinación e información con el Organismo de Certificación, indicadas en esta Sección.

Igualmente, y para la defensa de la validez y reconocimiento mutuo de certificados de la seguridad de los productos, el Organismo de Certificación trasladará al laboratorio las obligaciones requeridas, tanto al procedimiento de evaluación, como a los propios laboratorios de evaluación, en los acuerdos, convenios o contratos de reconocimiento mutuo en los que el solicitante de la certificación del producto quiera hacer valer la misma y el Organismo de Certificación opere.

Artículo 68. *Obligaciones de coordinación e información.*

El laboratorio deberá cumplir, en el desarrollo de sus trabajos de evaluación, con los requisitos de coordinación e información con el Organismo de Certificación que se incluyen en esta Sección.

Artículo 69. *Aprobación previa.*

1. El laboratorio de evaluación estará obligado a obtener aprobación previa, y por escrito, del Organismo de Certificación para comenzar los trabajos de evaluación.

En la aprobación previa deberá constar la asignación del responsable de la certificación del producto, por parte del Organismo de Certificación, a quien se dirigirán las comunicaciones relativas a la evaluación.

Esta obligación deberá estar recogida en los procedimientos de evaluación propios del laboratorio.

2. Dicha aprobación se solicitará por el laboratorio mediante escrito, al que se acompañará lo siguiente:

a) Plan detallado de la evaluación, con las fases, tareas y unidades de trabajo correspondientes, la asignación e identificación del personal afecto a la evaluación y su responsabilidad en la misma.

b) Copia del contrato, o documento similar, que regule las relaciones entre el laboratorio y el solicitante de la certificación, en las que el laboratorio incluirá, obligatoriamente, las cláusulas necesarias para el cumplimiento de los requisitos para la acreditación del laboratorio.

Artículo 70. *Inicio y fin de los trabajos de evaluación.*

El laboratorio de evaluación estará obligado a comunicar, al Organismo de Certificación, el comienzo y término de cada fase, actividad, acción y unidad de trabajo de la evaluación, según se definan en la metodología y procedimientos de evaluación a aplicar. En función de su relevancia, el Organismo de Certificación podrá rebajar este requisito a la comunicación de fases, actividades o hitos señalados.

Esta obligación deberá estar recogida en los procedimientos de evaluación propios del laboratorio.

Artículo 71. *Desviaciones del plan de evaluación.*

El laboratorio de evaluación estará obligado a comunicar, al Organismo de Certificación, las desviaciones con respecto al plan de evaluación, con análisis de las causas de la desviación, las medidas correctivas aplicadas por el laboratorio, y el nuevo plan de evaluación actualizado.

Esta obligación deberá estar recogida en los procedimientos de evaluación propios del laboratorio.

Artículo 72. *Dificultades en la evaluación.*

El laboratorio de evaluación estará obligado a comunicar, al Organismo de Certificación, cualquier dificultad surgida en la aplicación o interpretación de las normas utilizadas, así como cualquier dificultad que condicione el normal transcurso de una evaluación.

Esta obligación deberá estar recogida en los procedimientos de evaluación propios del laboratorio.

Artículo 73. *Informes de observación.*

El laboratorio estará obligado a remitir, al Organismo de Certificación, todos los informes de observación y de disconformidad emitidos e informará de su cierre, cuando ocurra, y de las medidas correctivas aplicadas por el solicitante de la certificación.

Esta obligación deberá estar recogida en los procedimientos de evaluación propios del laboratorio.

Artículo 74. *Información técnica adicional.*

El laboratorio de evaluación estará obligado a facilitar toda información técnica adicional que sea necesaria para el análisis, por parte del Organismo de Certificación, de la información de las evaluaciones, incluyendo acceso y formación sobre programas y sistemas de evaluación, elaborados o adquiridos por el laboratorio, así como aquellos métodos y técnicas de análisis de vulnerabilidades empleados.

Esta obligación deberá estar recogida en los procedimientos de evaluación propios del laboratorio.

Artículo 75. *Reuniones entre el solicitante y el laboratorio.*

El laboratorio de evaluación estará obligado a comunicar, e invitar a su asistencia, al Organismo de Certificación, de cuantas reuniones celebre dicho laboratorio con el solicitante de la certificación, con indicación de su naturaleza y objeto.

Esta obligación deberá estar recogida en los procedimientos de evaluación propios del laboratorio.

Artículo 76. *Reuniones de seguimiento.*

El laboratorio de evaluación estará obligado a atender cuantas reuniones de seguimiento convoque el Organismo de Certificación. Dichas reuniones se convocarán por el responsable de la certificación del producto del Organismo de Certificación, y serán atendidas por el personal requerido para explicar e interpretar la información de las evaluaciones objeto de seguimiento. En el caso de información de las evaluaciones elaborada por el laboratorio, se podrá requerir la asistencia a la reunión de los autores de la misma.

Esta obligación deberá estar recogida en los procedimientos de evaluación propios del laboratorio.

Artículo 77. *Puesta a disposición de dependencias y sistemas.*

El laboratorio de evaluación estará obligado a poner sus dependencias y sistemas de evaluación a disposición del Organismo de Certificación, para la realización, por parte del personal del mismo, de las tareas de verificación de la actividad de evaluación que se consideren oportunas.

Esta obligación deberá estar recogida en los procedimientos de evaluación propios del laboratorio.

CAPÍTULO IV

Acreditación de laboratorios

Sección 1.ª Acreditación

Artículo 78. *Acreditación.*

El Organismo de Certificación acreditará a los laboratorios solicitantes siguiendo el procedimiento establecido en la Sección 4.ª de este Capítulo y en base al cumplimiento de los requisitos establecidos en el Capítulo III.

Artículo 79. *Solicitantes.*

Pueden solicitar esta acreditación cualesquiera laboratorios de evaluación de la seguridad de los sistemas de información, con independencia de su naturaleza jurídica, pública o privada, sin más limitación que la de realizar su actividad de evaluación en territorio español.

Artículo 80. *Contenido de la acreditación.*

La acreditación de un laboratorio supone el reconocimiento de su competencia técnica, de la adecuación de la gestión de la seguridad del mismo a las particularidades de la evaluación de la seguridad de las Tecnologías de la Información, y de la consideración de los requisitos de coordinación e información al Organismo de Certificación, que permitirá a éste basar su dictamen de certificación de un producto, entre otros factores, en el informe de evaluación del laboratorio acreditado.

La acreditación de un laboratorio no presupone, sin embargo, aceptación incondicional de los resultados de la actuación de evaluación de un producto determinado. Dicha aceptación se otorgará tras el análisis inicial de la solicitud de certificación, mediante el seguimiento de la labor de evaluación y tras el análisis del correspondiente informe técnico de evaluación, tal y como se define en el Capítulo V.

Artículo 81. *Duración de la acreditación.*

La acreditación, una vez concedida, se mantiene de manera indefinida, salvo cambios en las condiciones que motivaron su concesión, incumplimiento de dichas condiciones o renuncia expresa del laboratorio. Para el mantenimiento de la acreditación, el Organismo de Certificación realizará, de oficio, las necesarias auditorías, inspecciones y análisis del laboratorio y de su actuación, conforme se regula en este Capítulo.

Sección 2.ª Alcance de la acreditación

Artículo 82. *Alcance de la acreditación.*

La acreditación se cualifica mediante el alcance, que limitará el reconocimiento de las actuaciones del laboratorio con relación al nivel de calificación de seguridad y con relación a las normas y niveles de evaluación.

Artículo 83. *Alcance con relación al nivel de calificación de seguridad.*

Con relación al nivel de calificación de seguridad se distinguen aquellos laboratorios con capacidad para manejar información y productos clasificados, de aquellos otros que operan en el régimen de la información y productos no clasificados.

Artículo 84. *Alcance con relación a las normas y niveles de evaluación.*

La certificación de la seguridad de los productos y sistemas de las Tecnologías de la Información puede requerir la evaluación de los mismos atendiendo a diferentes criterios, métodos y normas de evaluación.

Adicionalmente, dichas normas pueden distinguir niveles de evaluación y niveles de seguridad.

El Organismo de Certificación mantiene una relación actualizada de normas aplicables, según se establece en el Capítulo VI.

El laboratorio solicitante deberá indicar, en el alcance de la acreditación, aquellas normas y niveles, de la mencionada relación, en las que demuestra competencia técnica y experiencia acreditada.

Sección 3.ª Criterios de acreditación

Artículo 85. *Criterios generales.*

1. La competencia técnica del laboratorio solicitante se determinará, en primera instancia, por la correspondiente acreditación de esta competencia, conforme a lo regulado en la Ley 21/1992, de 16 de julio, de Industria, y en el Real Decreto 2200/1995, de 28 de diciembre, por el que se aprueba el Reglamento de la Infraestructura para la Calidad y Seguridad Industrial, y en base al cumplimiento, por parte del laboratorio, de la norma UNE-EN ISO/IEC 17025.

2. La acreditación de competencia técnica, que deberá ser concedida por una entidad de acreditación reconocida, ha de incluir, en su alcance, las normas de evaluación de la seguridad de los productos y sistemas de Tecnologías de la Información, aprobados por el Organismo de Certificación, y demás limitaciones requeridas por éste.

En particular, se reconocen las acreditaciones de competencia técnica emitidas por la Entidad Nacional de Acreditación, sin perjuicio de las acreditaciones emitidas por otras entidades de acreditación que satisfagan los requisitos establecidos en el Capítulo II del Reglamento de la Infraestructura para la Calidad y Seguridad Industrial.

3. Los requisitos adicionales, de gestión de la seguridad de la información de las evaluaciones, así como los de coordinación e información al Organismo de Certificación, se incluyen en el Capítulo III.

Los requisitos indicados en el párrafo anterior, se verificarán mediante la aplicación del procedimiento establecido en la siguiente Sección, sobre la base de una auditoría del laboratorio solicitante, que incluye el seguimiento de una evaluación de prueba bajo los procedimientos y requisitos del Organismo de Certificación.

Artículo 86. *Criterios complementarios.*

Para aquellos casos que lo requieran, los criterios generales mencionados podrán ser completados o precisados por otros complementarios de carácter técnico, específicos para cada tipo de producto a evaluar, criterios, métodos y normas de evaluación de cada acreditación, o modificación del alcance de la solicitada, recogidos y publicados en los correspondientes documentos del Organismo de Certificación.

Sección 4.ª Procedimiento de acreditación

Artículo 87. *Proceso de acreditación.*

Aquellos laboratorios que deseen ser acreditados por el Organismo de Certificación, deberán someterse al proceso de acreditación establecido en la presente Sección.

Artículo 88. *Solicitud de acreditación.*

La solicitud de acreditación deberá remitirse al Director del Organismo de Certificación adjuntando, como mínimo, la siguiente información, debidamente documentada:

a) Personalidad jurídica de la entidad solicitante, con su número de identificación fiscal.

b) Nombre del responsable del laboratorio y de la persona, o personas, con capacidad suficiente para obrar, que serán signatarias y, por tanto, responsables de la veracidad de las evaluaciones para las que el laboratorio solicita ser acreditado.

c) Compromiso de cumplir los requisitos de acreditación del Organismo de Certificación, indicados en el Capítulo III, así como declaración de disponibilidad para la realización de la auditoría y actividades derivadas del proceso de acreditación.

d) Relación y ubicación de las dependencias, delegaciones e instalaciones donde se realiza la actividad de evaluación de la seguridad de los productos y sistemas de las Tecnologías de la Información.

e) Alcance de la acreditación solicitada, indicando el nivel de calificación de seguridad y las normas y niveles de evaluación.

f) Relación y copia de los documentos del sistema de gestión de la calidad del laboratorio.

g) Relación y copia de los documentos del sistema de gestión de la seguridad del laboratorio.

h) Relación y copia de los manuales y procedimientos de evaluación del laboratorio.

i) Certificado de acreditación de la competencia técnica emitido por ENAC, o entidad de acreditación reconocida, según lo indicado en el artículo 85 o, en su caso, certificado de haber iniciado dicho proceso de acreditación con la entidad correspondiente.

j) Justificante del pago de las tasas de acreditación vigentes.

k) Alcance y descripción de las evaluaciones de prueba que el solicitante pretende llevar a cabo, bajo las condiciones y procedimientos de este esquema, para la demostración del cumplimiento de los requisitos de acreditación, y que han de ser de alcance igual, o superior, al de la acreditación solicitada.

Esta solicitud podrá presentarse en cualquiera de los lugares previstos en el artículo 38.4 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Artículo 89. *Modelo de solicitud de acreditación.*

Las solicitudes de acreditación de laboratorio se presentarán en los impresos establecidos al efecto, que estarán publicados en la dirección electrónica del Organismo de Certificación (http://www.oc.ccn.cni.es).

Artículo 90. *Subsanación y mejora de la solicitud de acreditación.*

A la recepción de la solicitud de acreditación, el Organismo de Certificación realizará una comprobación inicial de la información en ella contenida.

En caso de ser necesaria la subsanación o mejora de la solicitud de acreditación, se estará a lo dispuesto en el artículo 71 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Se admitirá durante la instrucción de la solicitud de acreditación la equivalencia del certificado de acreditación de la competencia técnica por certificado de encontrarse incurso en el proceso de acreditación de dicha competencia, siendo requisito definitivo para la acreditación del laboratorio, la certificación de su competencia técnica conforme a lo indicado en el artículo 85.

Artículo 91. *Notificación al solicitante.*

El Organismo de Certificación notificará al solicitante el inicio del procedimiento administrativo de acreditación, incluyendo en dicha notificación:

a) El nombre y datos de contacto del responsable del procedimiento de acreditación, que será igualmente responsable de la dirección de la auditoría inicial del cumplimiento de los requisitos para la acreditación.

b) La fecha propuesta de comienzo de la auditoría indicada.

Artículo 92. *Preparación de la auditoría.*

Los técnicos designados por el Organismo de Certificación, con carácter previo a la auditoría, realizarán un estudio preliminar de la documentación recibida junto con la solicitud, relativa a los sistemas de calidad, seguridad y evaluación del laboratorio solicitante.

Las conclusiones de dicho estudio, en términos de observaciones sobre el cumplimiento e identificación de disconformidades de los requisitos para la acreditación, se remitirán al solicitante con una antelación no inferior a un mes de la fecha de comienzo de la auditoría. Junto a dichas conclusiones, y a la vista del estudio realizado, el Organismo de Certificación

indicará la duración estimada de la auditoría, cuyo calendario definitivo se acordará en la fecha de comienzo de la misma.

El laboratorio solicitante podrá subsanar y mejorar la solicitud de acreditación en base a las conclusiones del estudio preliminar, con carácter previo a la realización de la auditoría.

Artículo 93. *Instrucción de la auditoría.*

La instrucción de la auditoría se realizará en tres fases: reunión inicial, desarrollo de la auditoría y reunión final.

a) Reunión inicial. En la fecha indicada por el Organismo de Certificación, se celebrará la reunión inicial de auditoría entre los representantes del laboratorio solicitante y el equipo auditor, designado por el Organismo de Certificación. En esta reunión se harán las presentaciones oportunas, se confirmará el plan y calendario de la auditoría y se revisarán las conclusiones del estudio preliminar de la solicitud.

b) Desarrollo de la auditoría. Durante esta fase se procederá a la observación del laboratorio solicitante durante la evaluación de prueba, y a la investigación del cumplimiento de los requisitos para la acreditación.

c) Reunión final. El equipo auditor se reunirá con los representantes de la entidad solicitante, con objeto de presentar un informe verbal de los resultados del desarrollo de la auditoría.

Artículo 94. *Informe del equipo auditor.*

El equipo auditor, en un plazo no superior a diez días contados desde la fecha de la reunión final de la auditoría, elaborará un informe con los resultados y con la información recopilada durante el desarrollo de la misma. Este informe será remitido al laboratorio solicitante para su conocimiento.

Artículo 95. *Audiencia previa.*

1. Una vez instruido el procedimiento de auditoría, se le pondrá de manifiesto al laboratorio solicitante y se le convocará a una reunión de audiencia previa a la resolución.

2. En dicha reunión, el Organismo de Certificación indicará la naturaleza, gravedad y consecuencias de las observaciones y disconformidades identificadas durante el procedimiento de auditoría, si las hubiere, con las implicaciones de las mismas en la resolución de la solicitud de acreditación.

3. El laboratorio solicitante, en un plazo no inferior a diez días ni superior a quince, podrá alegar y presentar los documentos y alegaciones que estime pertinentes.

4. Si antes del vencimiento del plazo, el laboratorio manifiesta su decisión de no efectuar alegaciones ni aportar nuevos documentos o justificaciones, se tendrá por realizado el trámite.

Artículo 96. *Resolución de la solicitud de acreditación.*

1. La resolución de la solicitud de acreditación se dictará de acuerdo con lo indicado en este artículo y en los plazos establecidos en el artículo 107, «Plazos y actos presuntos».

2. Esta resolución, de acuerdo con lo previsto en el artículo 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, podrá ser objeto de recurso potestativo de reposición ante el Director del Organismo de Certificación, cuya resolución pone fin a la vía administrativa, o ser impugnada directamente ante el orden jurisdiccional contencioso-administrativo.

3. La resolución de desestimación será motivada. La resolución de acreditación contendrá adicionalmente los siguientes extremos:

a) Alcance de la acreditación concedida.

b) La fecha en vigor de la acreditación y referencia a su vigencia.

Artículo 97. *Vigencia de la acreditación.*

1. La acreditación se concederá por plazo indefinido, salvo cambios en las condiciones que motivaron su concesión, incumplimiento de dichas condiciones o renuncia expresa del laboratorio.
2. Para el mantenimiento de la acreditación, el Organismo de Certificación realizará, de oficio, las necesarias auditorías, inspecciones y análisis del laboratorio y de su actuación, conforme a lo establecido en el presente Reglamento.

Artículo 98. *Certificación del producto evaluado en el proceso de auditoría.*

Las evaluaciones utilizadas como prueba, en el proceso de auditoría del laboratorio, podrán servir de base para la correspondiente certificación de la seguridad de los productos evaluados, conforme a lo indicado en el Capítulo V.

Sección 5.ª Seguimiento de la actividad de evaluación

Artículo 99. *Seguimiento continuo de la actividad de evaluación.*

El Organismo de Certificación, conforme al procedimiento de certificación de productos, establecido en el Capítulo V, realizará un seguimiento continuo de la actividad del laboratorio, a los efectos de la resolución de las solicitudes de certificación de productos.

Todas aquellas observaciones y disconformidades sobre los requisitos de acreditación del laboratorio, detectadas durante el seguimiento de las evaluaciones, serán comunicadas al laboratorio para su subsanación.

En el caso de disconformidad, o de no atender las observaciones realizadas, se estará a lo dispuesto en los artículos 104, 105 y 106.

Artículo 100. *Auditorías de seguimiento.*

1. De forma periódica, se realizarán auditorías de seguimiento a los laboratorios acreditados.
2. Los objetivos de las auditorías de seguimiento serán los siguientes:

a) Comprobar que la entidad ha respetado, durante el periodo transcurrido desde la última auditoría, los criterios establecidos para la concesión de la acreditación.
b) Verificar el cierre de las desviaciones detectadas en auditorías previas.
c) Examinar cualquier cambio en la organización, procedimientos y recursos de la entidad, para la realización de las actividades incluidas en el alcance de su acreditación.
d) Comprobar que se han respetado las obligaciones resultantes de la acreditación.
e) Comprobar la actividad de la entidad para el alcance acreditado.

3. La frecuencia de las auditorías se establecerá en función de los resultados de visitas previas.
4. La primera auditoría de seguimiento se programará en un plazo no superior a doce meses desde la fecha inicial de acreditación. Las siguientes auditorías de seguimiento se realizarán antes de transcurridos dieciocho meses desde la realización de la última visita.
5. Las auditorías de seguimiento se realizarán con el mismo grado de detalle y rigor que la auditoría inicial de acreditación.
6. En la instrucción y resolución de la auditoría de seguimiento se seguirá lo dispuesto en los artículos 93 y 94 y, en todo caso, se atendrá al procedimiento general administrativo.

Artículo 101. *Ampliación del alcance de una acreditación.*

Cuando un laboratorio, ya acreditado, desee ampliar el alcance de su acreditación deberá solicitar formalmente dicha ampliación. Para ello, deberá utilizar el formulario de solicitud correspondiente. Se aplicará el procedimiento indicado en el artículo 78 adaptado, según proceda, en función del volumen y carácter de dicha ampliación.

Artículo 102. *Notificación de cambios.*

1. El laboratorio deberá comunicar, al Organismo de Certificación, cualquier cambio que se proponga efectuar sobre las condiciones iniciales en que se concedió la acreditación y, en particular, los que afecten a lo siguiente:

a) Situación jurídica, comercial u organizativa del laboratorio.
b) Organización y gestión, cuando afecten a personal directivo o a puestos clave en la organización del laboratorio o de la empresa.
c) Políticas y procedimientos, cuando proceda.
d) Locales de ubicación del laboratorio.
e) Personal y otros recursos, cuando sean relevantes.
f) Documentos normativos incluidos en el alcance de la acreditación.

2. Ante una comunicación de cambio, el Organismo de Certificación procederá a su revisión y establecerá las actividades necesarias para el mantenimiento de la acreditación del laboratorio. Dichas actividades podrán consistir en acciones de auditoría, por parte del Organismo de Certificación, para comprobar el grado de cumplimiento de los requisitos de acreditación tras los cambios efectuados, así como en la actualización, por parte del laboratorio, de la documentación presentada en el proceso de acreditación.

Artículo 103. *Publicidad de las acreditaciones.*

El Organismo de Certificación podrá hacer pública la relación de laboratorios en proceso de acreditación, así como la de laboratorios acreditados incluyendo, en esta relación, la información del alcance de cada acreditación.

Sección 6.ª Formulación de observaciones, plazos y recursos

Artículo 104. *Formulación de observaciones y retirada de la acreditación.*

El incumplimiento de las obligaciones derivadas de la acreditación, por parte de la entidad titular de la misma, dará lugar a la adopción de medidas, por parte del Organismo de Certificación, contra la entidad incumplidora.

Las medidas irán en función de la gravedad del incumplimiento y podrán consistir en formulación de observaciones, retirada parcial o retirada total de la acreditación.

Artículo 105. *Actuaciones irregulares e incumplimientos.*

Se entenderá por actuaciones irregulares e incumplimientos leves, aquellas actuaciones que, sin adecuarse a lo establecido en el presente Reglamento, no afecten a la validez final de la actividad de evaluación de la entidad ni a la seguridad de terceros.

Las actuaciones irregulares y los incumplimientos leves serán objeto de observación, que podrá notificarse por los equipos de auditoría y seguimiento de las evaluaciones. El laboratorio deberá subsanar la causa que dio lugar a las observaciones, en el plazo de diez días.

Artículo 106. *Retirada de la acreditación.*

El incumplimiento reiterado de los requisitos de acreditación, o la no subsanación reiterada de las observaciones recibidas, darán lugar a la retirada, total o parcial, de la acreditación a la que se refiera.

La resolución de retirada de acreditación se dictará, de oficio, por el Organismo de Certificación.

La retirada de la acreditación obligará al solicitante al cese inmediato del uso de la condición de laboratorio acreditado, así como a la retirada de esta condición en todos los documentos o información en los que éste la haga manifiesta.

Artículo 107. *Plazos y actos presuntos.*

El plazo para resolver la solicitud de acreditación de laboratorio, y notificar la correspondiente resolución, será de seis meses. Este mismo plazo se aplicará a las solicitudes de ampliación del alcance de una acreditación previa.

A los efectos previstos en el artículo 43 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, las solicitudes de acreditación se entenderán estimadas de no recaer resolución expresa en los plazos establecidos en cada caso, con las salvedades y excepciones indicadas en dicho precepto.

Artículo 108. *Recursos.*

La actuación del Organismo de Certificación debe siempre atenerse a los principios generales de actuación recogidos en el artículo 3 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

De acuerdo con lo previsto en los artículos 116 y 117 de la citada Ley, así como en los artículos 10, 14 y 46 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, frente a la actuación del Organismo de Certificación, en materia de acreditación, se podrá interponer:

a) En el plazo de un mes, recurso potestativo de reposición ante el Director de dicho organismo, cuya resolución pone fin a la vía administrativa, o

b) Directamente, en el plazo de dos meses, recurso contencioso-administrativo, ante la Sala de dicha índole, del Tribunal Superior de Justicia de Madrid.

CAPÍTULO V

Certificación de productos y sistemas

Sección 1.ª Certificación

Artículo 109. *Certificación de seguridad de productos y sistemas.*

El Organismo de Certificación certificará la seguridad de los productos y sistemas de Tecnologías de la Información, siguiendo el procedimiento establecido en este Capítulo y tras considerar, entre otras pruebas de la instrucción del procedimiento, los informes de evaluación emitidos por los laboratorios acreditados conforme a lo establecido en el Capítulo IV, y realizados atendiendo a los criterios, métodos y normas de evaluación de la seguridad indicados en el Capítulo VI.

Artículo 110. *Reconocimiento de veracidad de propiedades de seguridad.*

La certificación de la seguridad de un producto o sistema de las Tecnologías de la Información supone el reconocimiento de la veracidad de las propiedades de seguridad de su correspondiente declaración de seguridad.

Artículo 111. *Valoración de idoneidad.*

La certificación de la seguridad de un producto o sistema no presupone declaración de idoneidad de uso en cualquier escenario o ámbito de aplicación. Para valorar la idoneidad de un producto o sistema deberán tenerse en cuenta otras circunstancias, incluidas las restricciones establecidas en su declaración de seguridad para la correcta interpretación del certificado.

Artículo 112. *Vigencia de la certificación.*

La certificación, una vez concedida, se mantiene de manera indefinida, salvo cambios en las condiciones que motivaron su concesión, tales como avances tecnológicos, aparición de nuevas vulnerabilidades explotables, incumplimiento de las condiciones de uso del certificado, cambios en el propio producto o renuncia expresa del solicitante. Para la

vigilancia de la vigencia de la certificación, el Organismo de Certificación realizará, de oficio, las necesarias auditorías, inspecciones y análisis del producto, de su entorno y del uso del certificado.

Sección 2.ª Alcance de la certificación

Artículo 113. *Alcance de la certificación.*

La certificación se limita mediante el correspondiente alcance, que incluye la definición del producto evaluado y las normas y niveles de evaluación.

El Organismo de Certificación, en la determinación del alcance, realizará la definición más precisa posible del mismo, al objeto de evitar confusión alguna entre el producto comercial y el producto evaluado, en el supuesto de que ambos no coincidan exactamente.

Artículo 114. *Alcance con relación al producto o sistema evaluado.*

La certificación deberá hacer referencia, e identificar inequívocamente, al producto evaluado, así como a su declaración de seguridad. Dicha declaración de seguridad también deberá contener la identificación precisa del producto evaluado, así como la especificación de su entorno de uso, incluyendo las amenazas previstas, políticas de seguridad e hipótesis aplicables al caso, además de los objetivos de seguridad del producto o sistema y la relación de requisitos de seguridad exigibles al mismo.

Los detalles de la declaración de seguridad podrán variar conforme a las normas aplicadas en la evaluación, pero toda declaración deberá ser un reflejo cierto, claro y preciso de las propiedades de seguridad del producto o sistema evaluado.

Artículo 115. *Alcance con relación a las normas y niveles de evaluación.*

La certificación incluirá en su alcance los criterios, métodos y normas de evaluación empleados en la evaluación del producto o sistema, así como el nivel que se haya alcanzado, de los definidos en cada norma, y la relación de interpretaciones e instrucciones técnicas aplicadas.

Sección 3.ª Criterios de certificación

Artículo 116. *Informe técnico de evaluación.*

La principal prueba en la instrucción del procedimiento de certificación es el Informe Técnico de Evaluación, emitido por el laboratorio acreditado y realizado cumpliendo con el procedimiento de certificación, establecido en la siguiente Sección.

Artículo 117. *Criterios complementarios.*

1. En el ejercicio de su función evaluadora, el Organismo de Certificación podrá, a su criterio, realizar análisis, pruebas, inspecciones y auditorías al laboratorio, al producto a evaluar y al solicitante de la certificación, en los aspectos y requisitos de garantía de seguridad que les sean de aplicación según los criterios y métodos de evaluación utilizados.

2. En particular, será atribución indelegable del Centro Criptológico Nacional el análisis, valoración y acreditación de los algoritmos y medios de cifra que utilice el producto a evaluar.

3. Igualmente, el seguimiento de la evaluación permitirá, al Organismo de Certificación, determinar el ajuste de la evaluación a los procedimientos derivados de las normas aplicables y, por tanto, el ajuste del Informe de Evaluación a las mismas.

Sección 4.ª Procedimiento de certificación

Artículo 118. *Proceso de certificación.*

Aquellos interesados que deseen certificar la seguridad de un producto o sistema de Tecnologías de la Información, deberán someterse al proceso establecido en la presente Sección.

Artículo 119. *Solicitud de certificación.*

1. La solicitud de certificación deberá remitirse al Director del Organismo de Certificación incluyendo en la misma, como mínimo, la siguiente información debidamente documentada:

a) Personalidad jurídica de la entidad solicitante, con su número de identificación fiscal.
b) Nombre del responsable del solicitante y de la persona, o personas, con capacidad suficiente para obrar, que serán signatarias y, por tanto, responsables de la veracidad de las evidencias y pruebas documentales aportadas.
c) Declaración responsable de conocer y aceptar los términos y requisitos aplicables a la certificación solicitada, incluyendo los derechos de acceso, publicación y limitación de la información de las evaluaciones por parte del Organismo de Certificación.
d) Identificación del laboratorio, acreditado por el Organismo de Certificación, que realizará la evaluación técnica de la seguridad del producto o sistema cuya certificación se solicita.
e) Relación y ubicación de las dependencias, delegaciones e instalaciones donde se realiza la actividad de desarrollo o integración del producto a evaluar.
f) Alcance de la certificación solicitada, indicando el producto a evaluar y su versión, así como las normas y niveles de evaluación aplicables.
g) Justificante del pago de las tasas de certificación en vigor.

Esta solicitud podrá presentarse en cualquiera de los lugares previstos en el artículo 38.4 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.
2. Junto a la solicitud de certificación, se remitirá al Organismo de Certificación la declaración de seguridad, o perfil de protección en su caso, del producto a evaluar y, cuando esto sea posible, una unidad, copia o ejemplar de este último.
3. Paralelamente a la solicitud, el solicitante gestionará con el laboratorio acreditado elegido, el plan detallado de la evaluación, así como el contrato o documento similar que regule las relaciones entre el laboratorio y el solicitante.

Artículo 120. *Modelo de solicitud de certificación.*

Las solicitudes de certificación de la seguridad de productos o sistemas de Tecnologías de la Información se presentarán en los impresos establecidos al efecto, que estarán publicados en la dirección electrónica del Organismo de Certificación (http://www.oc.ccn.cni.es).

Artículo 121. *Subsanación y mejora de la solicitud de certificación.*

1. A la recepción de la solicitud de certificación, el Organismo de Certificación realizará una comprobación inicial de la información en ella contenida.
2. En caso de ser necesaria la subsanación o mejora de la solicitud de certificación, se estará a lo dispuesto en el artículo 71 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.
3. Se podrá, igualmente, requerir al solicitante el suministro de unidades, copias o ejemplares adicionales del producto a evaluar, conforme a la naturaleza del mismo y a las necesidades derivadas de los criterios complementarios de certificación indicados en el artículo 117.
4. Será obligación del solicitante mantener actualizados el material y la documentación incluidos en la solicitud de certificación, en poder del Organismo de Certificación, en el caso de que alguno de éstos se modifique a resultas del proceso de evaluación correspondiente.

Artículo 122. *Notificación al solicitante.*

El Organismo de Certificación notificará al solicitante el inicio del procedimiento administrativo de certificación, incluyendo en dicha notificación el nombre y los datos de contacto del responsable del procedimiento de certificación.

Artículo 123. *Aprobación del comienzo de la evaluación.*

1. El laboratorio solicitará, al Organismo de Certificación, la autorización para comenzar la actividad de evaluación. La solicitud irá acompañada de:

a) El plan detallado de la evaluación, con las fases, tareas y unidades de trabajo correspondientes, la asignación e identificación del personal afecto a la evaluación y su responsabilidad en la misma.

b) La copia del contrato o documento similar que regule las relaciones entre el laboratorio y el solicitante de la certificación, en las que el laboratorio incluirá, obligatoriamente, las cláusulas necesarias para el cumplimiento de los requisitos de seguridad para la acreditación del laboratorio.

2. Para la resolución de la solicitud de autorización, se convocará una reunión con el laboratorio a la que asistirá el personal del laboratorio asignado a la evaluación y el equipo de certificación, designado por el Organismo de Certificación.

En esta reunión se harán las presentaciones oportunas y, por parte del laboratorio, se expondrá el plan y calendario de evaluación, así como los aspectos técnicos más relevantes de la misma.

3. El laboratorio deberá demostrar la adecuación y suficiencia de los medios materiales y humanos asignados a la evaluación, en particular, en lo referente a la formación del personal evaluador en los detalles del alcance de la certificación.

4. El Organismo de Certificación resolverá sobre la autorización del comienzo de la actividad de evaluación, incluyendo la designación del responsable del procedimiento de certificación.

Artículo 124. *Instrucción de la evaluación.*

1. La instrucción de la evaluación comenzará con el desarrollo de los trabajos de evaluación por parte del laboratorio, durante el cual, el Organismo de Certificación realizará el seguimiento de la actividad de evaluación del producto o sistema cuya certificación se ha solicitado.

Para la realización de este seguimiento, el Organismo de Certificación recibirá, del laboratorio, la información de la evaluación indicada en la Sección 3.ª del Capítulo III, a la vista de la cual convocará las reuniones de seguimiento que considere oportunas. En particular, será de especial atención el ajuste de la ejecución de la evaluación al correspondiente plan de evaluación.

2. La instrucción de la evaluación terminará con el Informe Técnico de Evaluación, que remitirá el laboratorio al Organismo de Certificación, en los siguientes casos:

a) Al término del plazo de evaluación.

b) Por solicitud del Organismo de Certificación. Dicha solicitud se podrá cursar cuando se haya superado, sin subsanar, el plazo de tres meses de cualquier observación o disconformidad, notificada al solicitante de la certificación, o a los tres meses de retraso no justificado del plan de evaluación.

Artículo 125. *Informe de certificación.*

El Organismo de Certificación, en un plazo no superior a treinta días contados desde la fecha de la recepción del Informe Técnico de Evaluación, elaborará un informe con los resultados y conclusiones de la evaluación, así como de la actividad de seguimiento, que será enviado al solicitante de la certificación para su conocimiento.

Artículo 126. *Audiencia previa a la resolución.*

1. Terminada la instrucción de la evaluación, se pondrá de manifiesto al solicitante de la certificación, convocándole a una reunión de audiencia previa a la resolución.

2. En dicha reunión, el Organismo de Certificación indicará la naturaleza, gravedad y consecuencias de las observaciones y disconformidades, identificadas durante la instrucción del expediente de certificación, si las hubiere, con las implicaciones de las mismas en la resolución de la solicitud de certificación.

3. El solicitante de la certificación, en un plazo no inferior a diez días ni superior a quince, podrá alegar y presentar los documentos y alegaciones que estime pertinentes.

4. Si antes del vencimiento del plazo, el solicitante manifiesta su decisión de no efectuar alegaciones ni aportar nuevos documentos o justificaciones, se tendrá por realizado el trámite.

Artículo 127. *Resolución de la solicitud de certificación.*

1. La resolución de la solicitud de certificación se dictará de acuerdo con lo indicado en este artículo, y en los plazos establecidos en el artículo 137, del presente Reglamento.

Esta resolución, de acuerdo con lo previsto en el artículo 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, podrá ser objeto de recurso potestativo de reposición ante el Director del Organismo de Certificación, cuya resolución pone fin a la vía administrativa, o ser impugnada directamente ante el orden jurisdiccional contencioso-administrativo.

2. Las resoluciones de desestimación serán motivadas. La resolución de certificación contendrá, adicionalmente, los siguientes extremos:

a) Alcance de la certificación concedida.

b) La fecha de la entrada en vigor de la certificación y referencia a su vigencia.

Artículo 128. *Vigencia de la certificación.*

La certificación se concederá por plazo indefinido, salvo cambios en las condiciones que motivaron su concesión, incumplimiento de dichas condiciones o renuncia expresa del solicitante.

Para el mantenimiento de la certificación, el Organismo de Certificación realizará, de oficio, las necesarias revisiones de su vigencia y actividades de vigilancia del uso del certificado, conforme a lo establecido en el artículo 129 siguiente.

Artículo 129. *Revisiones de vigencia.*

Cada dos años se realizará una revisión de la vigencia de cada certificado emitido. El objeto de dicha revisión es la comprobación de que el entorno de uso del producto certificado no ha sufrido variaciones, tales como cambios tecnológicos, aparición de vulnerabilidades o cualquier otro aspecto que pueda invalidar las hipótesis, análisis de riesgos y políticas de seguridad reflejadas en dicho entorno de uso.

La revisión de la vigencia de los certificados podrá dar lugar a la anulación del certificado, mediante resolución expresa del Director del Organismo de Certificación.

Sección 5.ª Seguimiento del uso de los certificados

Artículo 130. *Seguimiento continuo del uso del certificado.*

El Organismo de Certificación realizará un seguimiento continuo del uso de los certificados emitidos, mediante el análisis y registro de toda información comercial o técnica de la que tenga conocimiento y que haga referencia a la certificación emitida.

El incumplimiento de las condiciones de uso del certificado, reguladas en el Capítulo VII, podrá dar lugar a la anulación del certificado, mediante resolución expresa del Director del Organismo de Certificación.

Artículo 131. *Ampliación del alcance de la certificación.*

Cuando se desee ampliar el alcance de la certificación de un producto o sistema, el interesado solicitará formalmente dicha ampliación. Para ello deberá utilizar el formulario de solicitud correspondiente. Se aplicará el procedimiento de certificación, indicado en el Capítulo V, adaptado, según proceda, en función del volumen y carácter de dicha ampliación.

Artículo 132. *Notificación de cambios.*

El solicitante de la certificación deberá comunicar al Organismo de Certificación los cambios que identifique, relativos al entorno de seguridad del producto certificado, así como cualquier otro cambio fundamental que se produjese en las condiciones iniciales en que se concedió la certificación.

Artículo 133. *Publicidad de las certificaciones.*

El Organismo de Certificación podrá hacer pública la relación de productos en proceso de evaluación y la de productos certificados, incluyendo en esta relación la declaración de seguridad de los mismos, así como información derivada del informe de certificación establecido en el artículo 125.

Sección 6.ª Formulación de observaciones, plazos y recursos

Artículo 134. *Observaciones y retirada de la certificación.*

El incumplimiento, por un solicitante, de las obligaciones derivadas de la certificación dará lugar, en función de la gravedad de la infracción, a la formulación de observaciones o a la retirada de la certificación.

Artículo 135. *Actuaciones irregulares e incumplimientos.*

Las actuaciones irregulares y los incumplimientos leves, entendiéndose por tales los que no desvirtúen las restricciones y obligaciones derivadas del uso de la condición de producto certificado, serán objeto de observación, que se notificará, de oficio, al solicitante de la certificación.

El solicitante de la certificación deberá subsanar la causa de tales observaciones en un plazo de diez días.

Artículo 136. *Retirada de la certificación.*

1. La disconformidad sostenida, en relación con las restricciones y obligaciones del uso de la condición de producto certificado o con los requisitos para la certificación, así como la falta de subsanación de las observaciones recibidas, darán lugar a la retirada, total o parcial, de la certificación a la que se refiera.

2. La resolución de retirada de certificación se dictará, de oficio, por el Organismo de Certificación.

3. La retirada de la certificación obligará al solicitante al cese inmediato del uso de la condición de producto certificado, en todos los documentos o información en los que la haga manifiesta, y a la retirada del mercado de los productos así etiquetados.

Artículo 137. *Plazos y actos presuntos.*

1. El plazo para resolver la solicitud de certificación de productos, y notificar la correspondiente resolución, será de dos meses, contados a partir de la fecha de recepción del Informe Técnico de Evaluación del laboratorio.

Este mismo plazo se aplicará a las solicitudes de ampliación del alcance de una certificación previa.

2. El plazo para resolver la solicitud de comienzo de evaluación, y notificar la correspondiente resolución, será de un mes.

3. A los efectos previstos en el artículo 43 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo común, las solicitudes de certificación se entenderán estimadas de no recaer resolución expresa en los plazos establecidos en cada caso, con las salvedades y excepciones indicadas en dicho precepto.

Artículo 138. *Recursos.*

La actuación del Organismo de Certificación se atendrá a los principios generales de actuación recogidos en el artículo 3 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

De acuerdo con lo previsto en los artículos 116 y 117 de la citada Ley, y en los artículos 10, 14 y 46 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, frente a la actuación del Organismo de Certificación, en materia de certificación, los interesados podrán interponer:

a) En el plazo de un mes, recurso potestativo de reposición, ante el Director del dicho organismo, cuya resolución pone fin a la vía administrativa, o

b) Directamente, en el plazo de dos meses, recurso contencioso-administrativo, ante la Sala de dicha índole, del Tribunal Superior de Justicia de Madrid.

CAPÍTULO VI

Criterios y metodologías de evaluación

Artículo 139. *Estado del arte.*

El Organismo de Certificación certificará la seguridad de los productos y sistemas de Tecnologías de la Información conforme al estado del arte más avanzado en materia de evaluación de la seguridad. Dicho estado del arte se ha de combinar con el debido reconocimiento de los certificados emitidos.

A tal fin, el Organismo de Certificación exigirá a los laboratorios acreditados la realización de su actividad conforme a criterios, métodos y normas bien establecidos y reconocidos. Tales normas se podrán ver complementadas por interpretaciones o instrucciones técnicas emitidas por el Organismo de Certificación.

Artículo 140. *Normas de evaluación.*

1. El Organismo de Certificación, a los efectos de su utilización y cumplimiento por parte de los laboratorios, elevará a carácter de norma cualquier documento de orden técnico que sea de su interés, mediante la publicación del mismo en su dirección electrónica (http://www.oc.ccn.cni.es) y su comunicación a los laboratorios acreditados.

2. La publicación de una nueva norma, o la actualización de una existente, y la determinación de su entrada en vigor, se realizarán previa presentación a los laboratorios acreditados de las nuevas normas y de sus diferencias técnicas con respecto a las normas vigentes, a los efectos que pudieran derivarse sobre las acreditaciones en vigor.

3. Las normas relacionadas en el artículo 141 siguiente, se entienden de aplicación en su última versión disponible al comienzo de cada solicitud de certificación. No obstante lo anterior, se podrá consultar la relación de normas, criterios, metodologías y requisitos, así como su aplicabilidad, en la dirección electrónica del Organismo de Certificación (http://www.oc.ccn.cni.es).

Artículo 141. *Criterios de evaluación.*

Los criterios de evaluación serán los recogidos en las siguientes normas:

a) «Common Criteria for Information Technology Security Evaluation» (abreviado, CC).

b) ISO/IEC 15408, «Evaluation Criteria for IT Security».

c) «Information Technology Security Evaluation Criteria» (abreviado, ITSEC). Office for Official Publications of the European Communities.

Artículo 142. *Metodologías de evaluación.*

Las metodologías de evaluación serán las recogidas en las siguientes normas:

a) «Common Methodology for Information Technology Security Evaluation» (abreviado, CEM).

b) ISO/IEC 18045, «Methodology for IT Security Evaluation».

c) «Information Technology Security Evaluation Manual» (abreviado, ITSEM). Office for Official Publications of the European Communities.

Artículo 143. *Requisitos de seguridad específicos.*

Los requisitos de seguridad específicos serán los recogidos en la norma ISO/IEC 19790, «Requisitos de Seguridad para Módulos Criptográficos».

Artículo 144. *Interpretaciones e instrucciones técnicas.*

Se podrá consultar la relación de interpretaciones e instrucciones técnicas en vigor, de aplicación en este Esquema, en la dirección electrónica del Organismo de Certificación (http://www.oc.ccn.cni.es), agrupadas por la norma principal a la que afectan y sus versiones aplicables.

CAPÍTULO VII

Uso de la condición de laboratorio acreditado y de producto certificado

Artículo 145. *Referencia a la condición de laboratorio acreditado.*

La referencia a la condición de laboratorio acreditado, o el uso del distintivo correspondiente, en los informes emitidos como resultado de las actividades de evaluación amparadas por la acreditación, es el medio por el cual los laboratorios acreditados declaran públicamente el cumplimiento de todos los requisitos de acreditación en la realización de dichas evaluaciones.

Cualquier uso que no esté expresamente permitido en este Reglamento deberá ser consultado al Organismo de Certificación.

Artículo 146. *Informes derivados de la evaluación.*

1. La referencia a la condición de laboratorio acreditado debe ser utilizada en todos los informes emitidos como resultado de las actividades de evaluación, amparadas por la acreditación, como garantía del cumplimiento de los requisitos de dicha acreditación.

2. Cualquier informe o certificado que no incluya la referencia a la condición de laboratorio acreditado, no garantiza el cumplimiento de los requisitos de acreditación y, por tanto, no será aceptado por el Organismo de Certificación, como parte de una evaluación acreditada, ni podrá beneficiarse del reconocimiento de los certificados emitidos por el Organismo de Certificación.

3. En el caso de informes que incluyan, tanto datos amparados por la acreditación, como datos no amparados por la misma, se seguirán las siguientes reglas:

a) Se señalarán los datos no amparados por la acreditación mediante la utilización de un asterisco o similar. Asimismo, se deberá incluir en un lugar visible la siguiente leyenda: «Los ensayos/inspecciones marcados no están incluidos en el alcance de acreditación».

b) Cuando un informe de evaluación contenga interpretaciones, opiniones o cualquier otra información relativa a investigación, que no sea parte de la metodología de ensayo seguida en esa evaluación, se deberá incluir la siguiente advertencia: «Las opiniones, interpretaciones, etc., que se indican a continuación, están fuera del alcance de la acreditación del Organismo de Certificación».

Artículo 147. *Otros documentos de laboratorio acreditado.*

En documentos de tipo publicitario, folletos o anuncios relacionados con la actividad de evaluación acreditada, o en material de papelería (papel de cartas, impresos tales como facturas o pedidos, sobres, etc.), los laboratorios podrán usar la referencia a la condición de acreditado con las restricciones que se mencionan en el artículo 148.

Artículo 148. *Restricciones al uso de la condición de laboratorio acreditado.*

La referencia a la condición de laboratorio acreditado no se debe utilizar en los siguientes supuestos:

a) En informes o certificados que no contengan ningún dato obtenido de actividades acreditadas.

b) En documentos en los que no se identifique la organización a la que ha sido concedida la acreditación.

c) De forma que pueda sugerir que el Organismo de Certificación aprueba, acepta o, de alguna manera, se responsabiliza de los resultados contenidos en un informe o certificado (por ejemplo, mediante el uso de sellos con la referencia al Organismo de Certificación).

d) Cuando el laboratorio haya perdido su condición de acreditado, ya sea de forma voluntaria o por retirada de la acreditación.

e) En las tarjetas de visita del personal de los laboratorios acreditados.

f) En cualquier situación que pueda dar lugar a una interpretación incorrecta de la condición del laboratorio acreditado, o que pueda inducir a considerar actividades no acreditadas como cubiertas por la acreditación. Concretamente:

1.º Cuando se use en impresos (ofertas, cartas, presentaciones comerciales, material publicitario, páginas Web, etc.), que hagan referencia a actividades no acreditadas, se deberá incluir una mención, con el mismo tamaño de letra que el usado en el cuerpo del documento en cuestión, en la que se aclare este hecho (por ejemplo: «Las actividades recogidas en el presente escrito no están incluidas en el alcance de la acreditación del Organismo de Certificación»).

2.º Cuando se use en impresos (ofertas, cartas, presentaciones comerciales, material publicitario, etc.), que incluyan tanto actividades acreditadas como no acreditadas, su uso deberá ser tal, que permita al lector distinguir aquellas actividades que están acreditadas de las que no lo están.

3.º Cuando un laboratorio esté compuesto por varios emplazamientos distintos, y no todos ellos hayan sido acreditados, solamente aquellos que sí lo hayan sido podrán hacer uso de la referencia a la condición de acreditado. Cuando se emitan documentos comunes a todo el laboratorio se deberá incluir una cláusula que indique esta condición (por ejemplo: «Se encuentra disponible la lista de emplazamientos acreditados y sus alcances»).

4.º Cuando una organización acreditada pertenezca a otra mayor, no deberá existir confusión sobre cual de ellas está acreditada.

g) En cualquier otro supuesto que resulte abusivo, a juicio del Organismo de Certificación.

Artículo 149. *Uso de la condición de producto certificado.*

El uso del distintivo especificado en el artículo 155, o la referencia a la condición de producto certificado, es el medio por el cual los solicitantes de la certificación declaran, públicamente, el cumplimiento de todos los requisitos exigibles para dicha certificación, la conformidad con determinados perfiles de protección, en su caso, y el cumplimiento de las disposiciones legales aplicables.

Cualquier uso del certificado que no esté expresamente permitido en este Reglamento, deberá ser consultado al Organismo de Certificación.

Artículo 150. *Producto y documentación.*

La referencia a la condición de producto certificado debe ser utilizada en toda la documentación de administración y uso de dicho producto, y que se haya remitido como evidencia de la evaluación.

La referencia a la condición de producto certificado se incluirá también en el propio producto, siguiendo las reglas de marcado indicadas en el artículo 155.

Artículo 151. *Otros documentos de producto certificado.*

En documentos de tipo publicitario, folletos o anuncios relacionados con el producto certificado, así como en los contratos públicos y privados, licitaciones y documentación preparatoria, el titular de la certificación podrá usar la referencia a la condición de producto certificado con las restricciones que se mencionan en el artículo 152.

Artículo 152. *Restricciones al uso de la condición de producto certificado.*

La referencia a la condición de producto certificado no debe utilizarse en los siguientes supuestos:

a) Sin una referencia completa e inequívoca del alcance del certificado. Como mínimo se citará:

1.º Nombre y versión del producto evaluado.
2.º La norma utilizada para la evaluación y el nivel alcanzado en la misma (por ejemplo: ISO/IEC 15408 EAL2).
3.º Referencia a la declaración de seguridad del producto certificado, indicando el procedimiento para obtener una copia de la misma.

b) De forma que pueda sugerir que el certificado se aplica a todo un sistema o producto, cuando el producto evaluado es sólo una parte del mismo.
c) De forma que se sugieran propiedades de seguridad del producto certificado no reflejadas en su declaración de seguridad.
d) Cuando el certificado haya sido anulado por cualquier motivo.
e) En cualquier otro uso que resulte abusivo a juicio del Organismo de Certificación.

Artículo 153. *Otras obligaciones de la condición de producto certificado.*

La referencia a la condición de producto certificado obligará al solicitante de la certificación a:

a) Mantener registro de todas las reclamaciones presentadas al solicitante, relativas a la seguridad del producto certificado, y a tener esta información disponible para el Organismo de Certificación.
b) Tomar las acciones correctoras apropiadas con respecto a tales reclamaciones y a cualquier deficiencia encontrada en los productos, que afecten la conformidad con los requisitos para la certificación.
c) Documentar las acciones tomadas.

Artículo 154. *Distintivo de laboratorio acreditado.*

La condición de laboratorio acreditado puede complementarse mediante el uso del distintivo descrito a continuación (figura 2):

a) Color de fondo, diseño y detalles del escudo y tipo de letra, conforme a lo dispuesto en el Real Decreto 1465/1999, de 17 de septiembre, que establece los criterios de imagen institucional y regula la producción documental y el material impreso de la Administración General del Estado, y en la Orden de 27 de septiembre de 1999 por la que se aprueba el Manual de Imagen Institucional de la Administración General del Estado y se dictan normas de desarrollo del Real Decreto 1465/1999 citado (consultar página web «http://www.060.es»).
b) Círculo exterior de 180 unidades de medida de diámetro. Tamaño de letra nueve veces inferior al radio, esto es, de 20 unidades de medida.
c) Leyenda exterior, «ESQUEMA DE EVALUACIÓN Y CERTIFICACIÓN DE LA SEGURIDAD TI», sobre un arco de 270 grados, 140 unidades de medida de radio, y ángulo inicial de 135 grados, sentido negativo del texto.
d) Leyenda interior, «LABORATORIO ACREDITADO», sobre un arco de radio de 100 unidades de medida, iguales ángulos y recorrido que el exterior.
e) Escudo de España equidistante en sus aristas a la leyenda interior.
f) Si se reduce o amplía el distintivo, deberán respetarse las proporciones de este modelo.
g) La altura del distintivo no será inferior a 15 mm.

Figura 2. Distintivo de laboratorio acreditado

Artículo 155. *Distintivo de producto certificado.*

Los productos certificados deberán llevar un distintivo conforme a lo siguiente (figura 3):

a) Color de fondo, diseño y detalles del escudo y tipo de letra, conforme a lo dispuesto en el Real Decreto 1465/1999, de 17 de septiembre, que establece los criterios de imagen institucional y regula la producción documental y el material impreso de la Administración General del Estado, y en la Orden de 27 de septiembre de 1999 por la que se aprueba el Manual de Imagen Institucional de la Administración General del Estado y se dictan normas de desarrollo del Real Decreto 1465/1999 citado (consultar página web «http://www.060.es»).

b) Círculo exterior de 180 unidades de medida de diámetro. Tamaño de letra nueve veces inferior al radio, esto es, de 20 unidades de medida.

c) Leyenda exterior, «ESQUEMA DE EVALUACIÓN Y CERTIFICACIÓN DE LA SEGURIDAD TI», sobre un arco de 270 grados, 140 unidades de medida de radio, y ángulo inicial de 135 grados, sentido negativo del texto.

d) Leyenda interior, «PRODUCTO CERTIFICADO», sobre un arco de radio de 100 unidades de medida, iguales ángulos y recorrido que el exterior.

e) Escudo de España equidistante en sus aristas a la leyenda interior.

f) Si se reduce o amplía el distintivo, deberán respetarse las proporciones de este modelo.

g) La altura del distintivo no será inferior a 15 mm, excepto cuando esto no sea posible a causa del tipo de producto.

Figura 2. Distintivo de producto certificado con indicación del alcance

h) El distintivo deberá colocarse en el producto o en su placa informativa. Además, deberá colocarse en el embalaje, si existe, y en la documentación que le acompañe. En productos software, se mostrará el distintivo donde se haga referencia a la versión particular del producto.

i) El distintivo deberá colocarse de forma visible, legible e indeleble.

j) Se incluirá un elemento destinado a informar al usuario sobre el alcance de la certificación (norma y nivel aplicados en la evaluación).

§ 8

Orden ESS/775/2014, de 7 de mayo, por la que se crea el Comité de Seguridad de los Sistemas de Información de la Seguridad Social

Ministerio de Empleo y Seguridad Social
«BOE» núm. 117, de 14 de mayo de 2014
Última modificación: sin modificaciones
Referencia: BOE-A-2014-5111

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, reconoce el derecho de los ciudadanos a relacionarse con las administraciones públicas a través de medios electrónicos, comportando una obligación para éstas de promover las condiciones para que la libertad y la igualdad sean reales y efectivas, y la remoción de los obstáculos que impidan o dificulten su plenitud, lo que demanda incorporar las peculiaridades que exigen una aplicación segura de estas tecnologías.

Dicha ley determina que el Esquema Nacional de Seguridad tendrá por objeto establecer la política de seguridad en la utilización de medios electrónicos y estará constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, entiende por seguridad un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. Esta disposición reglamentaria obliga a todos los órganos superiores de las administraciones públicas a disponer formalmente de su política de seguridad, comprometiendo a todos los miembros de la organización.

En base a tales previsiones normativas, se dictaron la Orden TIN/3016/2011, de 28 de octubre, por la que se creó el Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Ministerio de Trabajo e Inmigración, y la Orden comunicada de la Ministra de Empleo y Seguridad Social, de 30 de julio de 2012, por la que se aprueba la Política de Seguridad de los Sistemas de Información del Ministerio de Empleo y Seguridad Social.

La Secretaría de Estado de la Seguridad Social, órgano superior del Ministerio de Empleo y Seguridad Social, ha establecido mediante Resolución de 2 de septiembre de 2013, de la Secretaría de Estado de la Seguridad Social, por la que se aprueba la política de seguridad en la utilización de medios electrónicos en la Administración de la Seguridad Social, su política de seguridad identificando unos claros responsables de velar por su cumplimiento. La proliferación de los sistemas de información de los organismos adscritos y de los órganos dependientes de la Secretaría de Estado y la interconexión entre ellos, hace aconsejable la creación de un Comité de Seguridad de los Sistemas de Información en el ámbito de la Seguridad Social, como órgano colegiado con funciones de coordinación de aquéllos y de propuesta y aprobación de las medidas conducentes al cumplimiento de la política de seguridad a que obliga el Esquema Nacional de Seguridad.

En la tramitación de esta orden se ha obtenido el informe favorable del Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Ministerio de Empleo y Seguridad Social.

En su virtud, con la aprobación previa del Ministro de Hacienda y Administraciones Públicas, dispongo:

Artículo 1. *Creación y adscripción del Comité de Seguridad de los Sistemas de Información de la Seguridad Social.*

Se crea el Comité de Seguridad de los Sistemas de Información de la Seguridad Social (en adelante CSISS) como órgano colegiado adscrito a la Secretaría de Estado de la Seguridad Social.

Artículo 2. *Funciones.*

El CSISS coordinará todas las actividades relacionadas con la seguridad de los sistemas de información en el ámbito de la Secretaría de Estado y se comunicará con el Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Ministerio de Empleo y Seguridad Social (en adelante CSTIC), ejerciendo las siguientes funciones:

1. Definir y elevar para su aprobación al CSTIC los planes estratégicos, líneas de actuación y objetivos en materia de seguridad en la Secretaría de Estado de la Seguridad Social, siempre alineados con la misión y objetivos de la organización.
2. Garantizar la divulgación de la política de seguridad en el ámbito de la Secretaría de Estado de la Seguridad Social.
3. La aprobación y seguimiento de las normas y procedimientos en materia de seguridad que afecten transversalmente a la Administración de la Seguridad Social.
4. Establecer, cuando sea posible, criterios comunes de actuación en todos los órganos directivos de la organización para el cumplimiento de las normas o procedimientos en materia de seguridad de la información que sean de aplicación.
5. Revisar el estado global de la seguridad en cada uno de los organismos adscritos y órganos y unidades dependientes orgánicamente de la Secretaría de Estado, y elevar los informes pertinentes al CSTIC cuando sea necesario.
6. Trasladar las directrices que sean establecidas desde el CSTIC a cada uno de los órganos directivos y garantizar su cumplimiento.
7. Actualizar y asignar las funciones y obligaciones de cada uno de los responsables definidos en la política de seguridad en la utilización de medios electrónicos en la Administración de la Seguridad Social.
8. Promover las líneas de trabajo para una adecuada concienciación y formación en materia de seguridad para el personal de la Secretaría de Estado de la Seguridad Social.
9. Ser informado, deliberar e intercambiar información con los organismos adscritos y órganos y unidades dependientes orgánicamente de la Secretaría de Estado y que sean responsables de ficheros con datos personales para tratar y asesorar sobre las medidas de seguridad técnica aplicables en los sistemas y servicios que les afecten y que utilicen tecnologías de la información y comunicaciones.

Artículo 3. *Composición.*

El CSISS estará compuesto por los siguientes miembros:

1. Presidente: El Secretario de Estado de la Seguridad Social o persona que le sustituya.
2. Vocales: un representante designado por los titulares de cada uno de los siguientes órganos:

a) Gabinete de la Secretaría de Estado de la Seguridad Social.
b) Dirección General de Ordenación de la Seguridad Social.
c) Intervención General de la Seguridad Social.
d) Instituto Nacional de la Seguridad Social.
e) Tesorería General de la Seguridad Social.
f) Instituto Social de la Marina.
g) Servicio Jurídico de la Administración de la Seguridad Social.

h) Gerencia de Informática de la Seguridad Social.

Estos vocales deberán tener rango de subdirector general o asimilado, entendiéndose también por tales quienes ejerzan competencias en materia de seguridad de los sistemas de información en los órganos anteriores.

3. Secretaría: Con voz y sin voto, será designada por la Gerencia de Informática de la Seguridad Social.

Artículo 4. *Funcionamiento.*

El CSISS se reunirá con carácter ordinario como mínimo tres veces al año o, con carácter extraordinario, cuando el Presidente lo considere necesario.

En caso de ser necesario, y por invitación del Presidente del CSISS, podrán asistir en calidad de asesores, con voz pero sin voto, las personas que se estimen convenientes.

En todo caso, se aplicará con carácter supletorio lo dispuesto en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Disposición adicional única. *No incremento del gasto público.*

La creación y el funcionamiento del Comité de Seguridad de los Sistemas de Información de la Seguridad Social serán atendidos con los medios personales, técnicos y presupuestarios asignados a la Secretaría de Estado de la Seguridad Social.

Disposición final única. *Entrada en vigor.*

La presente orden entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

§ 9

Orden TES/369/2023, de 10 de abril, por la que se aprueba la Política de Seguridad de la Información y de los Servicios en el ámbito de la administración digital del Ministerio de Trabajo y Economía Social y se crea el Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Departamento

Ministerio de Trabajo y Economía Social
«BOE» núm. 91, de 17 de abril de 2023
Última modificación: sin modificaciones
Referencia: BOE-A-2023-9290

El marco de relación entre la Administración Pública y los ciudadanos a través de los medios electrónicos se encuentra establecido en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Por su parte, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público define, en su artículo 156, el objeto del Esquema Nacional de Seguridad (ENS) y lo incorpora como parte esencial en la configuración del archivo electrónico de los documentos regulado en el artículo 46 y en el régimen de relaciones electrónicas y transferencias de tecnología entre las Administraciones Públicas, tal como establece su artículo 158.

Ambas normas han sido objeto de desarrollo mediante el Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.

La administración digital debe ser confiable para que los ciudadanos realicen los trámites administrativos correspondientes con total seguridad y fiabilidad. Para ello, el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, persigue alcanzar una protección adecuada de la información tratada y de los servicios prestados por las entidades de su ámbito de aplicación, con objeto de asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos que gestionen en el ejercicio de sus competencias.

En particular, el artículo 12.3 del citado Real Decreto 311/2022, de 3 de mayo, establece que, en la Administración General del Estado, cada ministerio contará con su política de seguridad, que aprobará la persona titular del Departamento.

La política de seguridad de la información constituye el marco de referencia orientado a facilitar la definición, gestión, administración e implementación de los mecanismos y procedimientos de seguridad establecidos en el ENS.

Además, la política de seguridad de la información debe ser coherente con lo establecido en el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva

95/46/CE (Reglamento General de Protección de Datos) y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

En el ámbito del Ministerio de Trabajo y Economía Social se debe garantizar la seguridad como un proceso integral de cada etapa del ciclo de vida de cada sistema de información, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Además, el sistema de información debe estar preparado para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con lo que prevé el Esquema Nacional de Seguridad.

Mediante el Real Decreto 2/2020, de 12 de enero, por el que se reestructuran los departamentos ministeriales, fue creado el Ministerio de Trabajo y Economía Social. Posteriormente, se aprobaron el Real Decreto 139/2020, de 28 de enero, por el que se establece la estructura orgánica básica de los departamentos ministeriales, y el Real Decreto 499/2020, de 28 de abril, por el que se desarrolla la estructura orgánica básica del Ministerio de Trabajo y Economía Social, y se modifica el Real Decreto 1052/2015, de 20 de noviembre, por el que se establece la estructura de las Consejerías de Empleo y Seguridad Social en el exterior y se regula su organización, funciones y provisión de puestos de trabajo.

El marco normativo vigente en el ámbito de la prestación de servicios electrónicos a los ciudadanos, en materia de política de seguridad de la información y de protección de datos personales, así como la actual organización administrativa determinan la necesidad de dictar esta orden por la que se aprueba la política de seguridad de la información y de los servicios en el ámbito de la administración digital del Ministerio de Trabajo y Economía Social y se crea, en este Departamento, el Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones.

Esta orden cumple con los principios de buena regulación, de necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia y eficiencia recogidos en el artículo 129 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

En primer lugar, en virtud de los principios de necesidad y eficacia, esta iniciativa normativa está justificada por las razones expuestas y es el instrumento más adecuado para dar cumplimiento al mandato contenido en el artículo 12.3 del citado Real Decreto 311/2022, de 3 de mayo. Además, se ajusta al principio de proporcionalidad, en tanto que la norma contiene la regulación imprescindible para atender sus objetivos. Se garantiza el principio de seguridad jurídica, en tanto que la norma es coherente con el resto del ordenamiento jurídico y, en particular, con el marco regulatorio en el ámbito de la política de seguridad de la información. Cumple con el principio de transparencia, ya que identifica claramente su propósito y, al tratarse de una norma organizativa su tramitación no ha requerido de la consulta pública previa ni de los trámites de audiencia e información pública. Finalmente, es también adecuada al principio de eficiencia, ya que no impone cargas administrativas.

La orden se ha desarrollado también en el marco de lo dispuesto en la disposición adicional primera de la Ley Orgánica de Protección de Datos Personales y Garantía de Derechos Digitales (LOPD) y del artículo 32 del Reglamento UE 2016/679, del Parlamento Europeo y del Consejo (RGPD) en orden a aplicar las medidas de seguridad al tratamiento de datos personales.

En el proceso de su tramitación, ha sido informada por la Agencia Española de Protección de Datos y por la Comisión Ministerial de Administración Digital del Ministerio de Trabajo y Economía Social.

En su virtud, con la aprobación previa de la Ministra de Hacienda y Función Pública, dispongo:

Artículo 1. *Objeto y ámbito de aplicación.*

1. El objeto de esta orden ministerial es la aprobación de la Política de Seguridad de la Información y de los Servicios (en adelante Política de Seguridad o PSI), en el ámbito de la Administración Digital del Ministerio de Trabajo y Economía Social, así como la creación del Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Ministerio de Trabajo y Economía Social y la regulación de su composición, funcionamiento y funciones.

2. La Política de Seguridad establece las orientaciones o directrices que rigen la actuación en el Ministerio de Trabajo y Economía Social, de las personas y entidades, en relación con la seguridad de los sistemas de información; entendiendo que un Sistema de Información es un conjunto organizado de recursos (físicos, lógicos, de comunicación, de datos, procedimientos y personas) que permite conseguir las especificaciones funcionales establecidas para el Departamento. La Política de Seguridad aprobada en esta orden ministerial se aplicará a todos los sistemas de información del Ministerio de Trabajo y Economía Social.

La PSI es de obligado cumplimiento para todo el personal que acceda a los sistemas de información y a la información del Departamento y para los órganos superiores y directivos del Ministerio de Trabajo y Economía Social y de sus organismos públicos adscritos, que no tengan establecida su propia política de seguridad.

En caso de discrepancia con las políticas de seguridad que pudieran estar definidas de manera específica para tales órganos y organismos públicos, prevalecerá la definida en esta orden ministerial.

Artículo 2. *Misión del Departamento.*

Corresponde al Ministerio de Trabajo y Economía Social la propuesta y ejecución de la política del Gobierno en materia de empleo, de relaciones laborales, de economía social y de responsabilidad social de las empresas, de acuerdo con lo establecido en el Real Decreto 499/2020, de 28 de abril, por el que se desarrolla la estructura orgánica básica del Ministerio de Trabajo y Economía Social, y se modifica el Real Decreto 1052/2015, de 20 de noviembre, por el que se establece la estructura de las Consejerías de Empleo y Seguridad Social en el exterior y se regula su organización, funciones y provisión de puestos de trabajo.

Artículo 3. *Marco normativo.*

1. El marco normativo en que se desarrollan las actividades del Ministerio de Trabajo y Economía Social en el ámbito de la prestación de los servicios electrónicos a la ciudadanía, sin perjuicio de la legislación específica, está integrado fundamentalmente por las siguientes disposiciones:

a) Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

b) Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

c) Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

d) Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

e) Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

f) Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.

g) Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.

h) Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

i) Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

j) Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en al ámbito de la Administración Electrónica.

k) Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

l) Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional.

2. También forman parte del marco normativo las restantes normas aplicables a la administración electrónica del Departamento derivadas de las anteriores y publicadas en las sedes electrónicas dentro del ámbito de aplicación de la PSI.

3. El Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Ministerio de Trabajo y Economía Social mantendrá actualizado dicho marco normativo, especialmente las instrucciones técnicas de seguridad, de obligado cumplimiento, esenciales para lograr una adecuada, homogénea y coherente implantación de los requisitos y medidas recogidos en el Esquema Nacional de Seguridad.

Artículo 4. *Principios de la Política de Seguridad.*

1. La política de seguridad aplicará los principios básicos que se establecen en el ENS en el ámbito de la Administración electrónica, de acuerdo con el interés general, naturaleza y complejidad de la materia regulada, permitiendo una protección adecuada de la información y de los servicios.

2. Atendiendo al ENS, el Ministerio de Trabajo y Economía Social implementará diversas medidas de seguridad proporcionales a la naturaleza de la información y de los servicios a proteger, teniendo en cuenta la categoría de los sistemas afectados bajo los siguientes principios:

a) Protección de datos personales. Se adoptarán las medidas técnicas y organizativas destinadas a garantizar el nivel de seguridad exigido por la normativa vigente en relación con el tratamiento de datos de carácter personal.

b) Alcance estratégico. La seguridad de la información en el que deberá contar con el compromiso y apoyo de todos los niveles directivos de forma que pueda estar coordinada e integrada con el resto de las iniciativas estratégicas del Departamento para conformar un todo coherente y eficaz.

c) Seguridad Integral. La seguridad constituirá un proceso integral compuesto por todos los elementos técnicos, humanos, materiales y organizativos relacionados con el sistema basado en la mejora continua de todos ellos y del proceso en sí mismo.

d) Análisis y gestión de riesgos: Todos los sistemas afectados por la PSI, así como todos los tratamientos de datos personales, serán objeto de un análisis de riesgos que evalúe las amenazas y los riesgos a los que están expuestos. Este análisis, que deberá ajustarse, en todo caso, a un criterio de proporcionalidad a los riesgos potenciales y la criticidad y valor de la información y de los servicios afectados, y de acuerdo con los artículos 24, 25 y 32 del RGPD, el artículo 28 de la LOPD y 3 del RD 311/2022, cuando el sistema de información trate datos personales, se realizará:

1.º Regularmente, al menos una vez al año, revisando la situación del Sistema de Información para determinar si se han producido cambios que requieran una actualización en materia de seguridad.

2.º Cuando cambie la información manejada o los servicios prestados de manera significativa.

3.º Cuando ocurra un incidente grave de seguridad o se detecten vulnerabilidades graves.

e) Prevención, reacción, recuperación y mejora continua. Se implementará un proceso integral de prevención, reacción y recuperación frente a incidentes de seguridad con procedimientos de detección, análisis, comunicación, resolución y registro de las actuaciones para la mejora continua de la seguridad de los sistemas, designando un punto de contacto para las comunicaciones con respecto a incidentes detectados y estableciendo protocolos para el intercambio de información relacionada con el incidente, incluyendo las comunicaciones con los Equipos de Respuesta a Emergencias (CERT).

f) Líneas de defensa. Se implementará una estrategia de protección basada en múltiples capas, constituidas por medidas organizativas, físicas y lógicas, de tal forma que cuando una de las capas falla, el sistema implementado permitirá ganar tiempo para una reacción

adecuada frente a los incidentes que no han podido evitarse; reducir la probabilidad de que el sistema sea comprometido en su conjunto y minimizar el impacto final sobre el mismo.

g) Reevaluación periódica e integridad y actualización del sistema. Se implementarán controles y evaluaciones regulares y periódicas de la seguridad (de forma interna o con la ayuda de terceros) para conocer en todo momento el estado de la seguridad de los sistemas con el objeto de adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección, llegando incluso a un replanteamiento de la seguridad, si fuese necesario.

h) Función diferenciada: El Ministerio de Trabajo y Economía Social organizará su seguridad comprometiendo a todos los miembros del Departamento mediante la designación de diferentes roles de seguridad con responsabilidades claramente diferenciadas, tal y como se recoge en el artículo 6. Estos controles, así como los roles y responsabilidades de seguridad de todo el personal, estarán claramente definidos y documentados.

En los supuestos de tratamientos de datos personales se identificará además a la persona, organismo o unidad responsable del tratamiento y, en su caso, al encargado de tratamiento, de acuerdo con los dispuesto en el artículo 4, apartados 7 y 8 del RGPD.

Artículo 5. *Requisitos de la seguridad de la información.*

Tal y como establece el ENS, la política de seguridad debe desarrollarse aplicando una serie de requisitos mínimos:

a) Organización e implantación del proceso de seguridad. La seguridad deberá comprometer a todo el personal del Ministerio de Trabajo y Economía Social.

b) Análisis y gestión de los riesgos. Se realizará una gestión de los riesgos consistente en un proceso de identificación, análisis, evaluación y tratamiento a los que el sistema esté expuesto. Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.

Cuando un sistema de información trate datos personales, la persona responsable o encargada del tratamiento, asesorada por la persona delegada de protección de datos, realizará un análisis de riesgos conforme al artículo 24 del Reglamento General de Protección de Datos y, en los supuestos de su artículo 35, una evaluación de impacto en la protección de datos.

El análisis y la gestión deberá realizarse de acuerdo con las previsiones del artículo 15 de la presente orden ministerial, adaptando los criterios de determinación del riesgo en el tratamiento de los datos conforme a lo establecido en el artículo 32 del RGPD y, en caso necesario, estableciendo niveles de seguridad más altos.

c) Gestión de personal y profesionalidad. Se establecerá un programa de concienciación continua anual para formar a todos los empleados públicos que prestan servicio en su ámbito, en particular, a los de nueva incorporación. Del mismo modo, las personas con responsabilidad concreta en el uso, operación o administración de sistemas TIC recibirán formación específica para el manejo seguro de los sistemas en la medida en que la necesitan para realizar su trabajo. La formación será obligatoria antes de asumir una nueva responsabilidad, tanto si es la primera asignación como si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

d) Autorización y control de los accesos. Se implementarán mecanismos de control de acceso al sistema general de información, limitándolos a los estrictamente necesarios y debidamente autorizados. Los sistemas de información individuales se diseñarán de forma que garanticen la seguridad por defecto, proporcionando la mínima funcionalidad requerida para alcanzar los objetivos y priorizando el uso sencillo, de tal forma que una utilización insegura requiera, en todo caso, de un acto consciente por parte del usuario. Tales sistemas de información individuales serán solo accesibles por las personas o desde emplazamientos o equipos autorizados, pudiendo exigirse, en su caso, restricciones de horario y puntos de acceso facultados.

e) Protección de las instalaciones. Se implementarán mecanismos de control de acceso físico, previniendo los accesos físicos no autorizados, así como los daños a la información y a los recursos, mediante perímetros de seguridad, controles físicos y protecciones generales en áreas.

f) Adquisición de productos. Ante cualquier adquisición, el Ministerio de Trabajo y Economía Social tendrá en cuenta que dichos productos tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen.

g) Seguridad por defecto. Los sistemas deberán diseñarse y configurarse de forma que garanticen la seguridad por defecto. El sistema proporcionará la mínima funcionalidad requerida para que la organización alcance sus objetivos. Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que solo son accesibles por las personas, o desde emplazamientos o equipos, autorizados.

Cuando el sistema afecte a datos personales, la adopción de medidas de seguridad por defecto y desde el diseño deberá realizarse de acuerdo con los artículos 24 y 25 del RGPD.

h) Integridad y actualización del sistema. Todo elemento físico o lógico requerirá autorización formal previa a su instalación en el sistema. Se deberá conocer en todo momento el estado de seguridad de los sistemas, en relación a las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos.

i) Protección de la información almacenada y en tránsito. Se implementarán mecanismos para proteger la información almacenada o en tránsito, especialmente cuando esta se encuentra en entornos inseguros (portátiles, tablets, soportes de información, redes abiertas, etc.). Los sistemas dispondrán de los medios de protección de la información almacenada y en tránsito (copias de seguridad y otros mecanismos necesarios), que garanticen la continuidad de las operaciones en caso de pérdida de los medios habituales de trabajo.

j) Prevención ante otros sistemas de información interconectados. La estrategia de protección protegerá el perímetro, en particular, si se conecta a redes públicas. En todo caso, analizará los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas y se controlará su punto de unión.

k) Registro de actividad. Se habilitarán registros de la actividad de las personas usuarias reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de las personas afectadas, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral y demás disposiciones que resulten de aplicación.

l) Incidentes de seguridad. Se establecerá un sistema de detección y reacción frente a código dañino.

m) La gestión de incidentes que afecten a datos personales tendrá en cuenta lo dispuesto en el RGPD, la LOPD, en especial su disposición adicional primera, así como el resto de la normativa de aplicación.

Se deberán implementar medios organizativos y materiales que, en los supuestos de violación de la seguridad de los datos personales, garanticen la notificación a la autoridad de control, la documentación del incidente y la comunicación a los interesados, en su caso, requiriendo para ello la implicación del delegado de protección de datos.

n) Continuidad de la actividad. Los sistemas de información del Ministerio de Trabajo y Economía Social dispondrán de copias de seguridad y establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales de trabajo.

o) Mejora continua del proceso de seguridad. El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua.

p) Auditoría de la seguridad. Se promoverá las auditorías de los sistemas de información de manera regular, al menos cada dos años, para que se verifique el cumplimiento de los requerimientos del Esquema Nacional de Seguridad, siguiendo la normativa vigente en función de la categoría de cada sistema de información.

Artículo 6. *Estructura organizativa para la gestión de la seguridad.*

La estructura organizativa para la gestión de la seguridad de los sistemas de información del Ministerio de Trabajo y Economía Social está compuesta por:

a) El Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones (COSTIC).
b) Las personas responsables de los sistemas de información.
c) Las personas responsables de la información y de los servicios.
d) Las personas responsables de la seguridad.
e) La persona designada como delegada de protección de datos.
f) Las personas responsables del tratamiento de datos personales.
g) Las personas encargadas del tratamiento de datos personales.
h) Las personas responsables de la prestación de los servicios TIC.

Artículo 7. *El Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Ministerio de Trabajo y Economía Social.*

1. Se crea el Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Ministerio de Trabajo y Economía Social, en adelante COSTIC, como órgano colegiado de carácter transversal, adscrito a la Subsecretaría de Trabajo y Economía Social con la siguiente composición:

a) Presidencia: La persona titular de la Subsecretaría de Trabajo y Economía Social.
b) Vicepresidencia: La persona titular de la Dirección del Gabinete Técnico de la Subsecretaría.
c) Vocalías:

1.º Un representante designado por la persona titular de la Secretaría de Estado de Empleo y Economía Social, con rango mínimo de subdirector general o asimilado.
2.º Un representante designado por la persona titular de la Subsecretaría de Trabajo y Economía Social, con rango mínimo de subdirector general o asimilado.
3.º La persona titular de la Subdirección General de Tecnologías de la Información y Comunicaciones, que, además, actuará como secretaria del COSTIC.
4.º La persona responsable de la seguridad del Ministerio.
5.º La persona responsable de la seguridad del Servicio Público de Empleo Estatal (SEPE).
6.º La persona responsable de la seguridad del Fondo de Garantía Salarial (FOGASA).
7.º La persona responsable de la seguridad del Instituto Nacional de Seguridad y Salud en el Trabajo (INSST).
8.º La persona responsable de la seguridad del Organismo Estatal de la Inspección de Trabajo y Seguridad Social (OEITSS).

2. La persona designada como delegada de protección de datos participará con voz, pero sin voto, en las reuniones del COSTIC, cuando en el mismo vayan a abordarse cuestiones relacionadas con el tratamiento de datos de carácter personal, así como siempre que se requiera su participación.
3. En casos de vacante, ausencia, enfermedad, abstención, recusación u otra causa legal, la persona a la que corresponda la Presidencia será sustituida por la persona titular de la Vicepresidencia. La persona que ostente la Secretaría del órgano será sustituida, en su caso, por el vocal designado por la persona titular de la Subsecretaría. En el caso de las vocalías, las personas que las desempeñen serán sustituidas por quienes designe el órgano que ha designado a las titulares.
4. Con carácter opcional, en función de los asuntos a tratar, otros miembros del Ministerio de Trabajo y Economía Social podrán incorporarse a las labores del Comité, incluyendo las personas responsables de la información, de los servicios, de los sistemas de información y grupos de trabajo especializados, ya sean de carácter interno, externo o mixto.

Artículo 8. *Funciones del Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Ministerio de Trabajo y Economía Social.*

Al COSTIC le corresponden las siguientes funciones:

a) Proponer revisiones y actualizaciones de la Política de Seguridad y de las normas de seguridad.

b) Mantener actualizado el marco normativo aplicable a la seguridad de los sistemas de información.

c) Proponer planes de mejora de la seguridad de los sistemas de información, que podrán contemplar la aprobación, revisión y mejora de los planes estratégicos, los planes directores, los procedimientos, las normas y las líneas de actuación del Departamento en materia de seguridad de los sistemas de información, con su dotación presupuestaria correspondiente, priorizando las actuaciones en materia de seguridad, cuando los recursos sean limitados.

d) Promover, aprobar, revisar y mejorar las políticas de auditoría, en especial del ENS y de la protección de datos personales, de las unidades del Departamento.

e) Aprobar las declaraciones de aplicabilidad y conformidad con el ENS.

f) Realizar un seguimiento de los principales riesgos residuales e incidentes de seguridad y recomendar posibles actuaciones respecto a ellos.

g) Elaborar programas de formación destinados a formar y sensibilizar al personal en materia de seguridad de la información y, en particular, en materia de protección de datos de carácter personal.

h) Definir los mecanismos y resolver los conflictos entre las personas con roles de seguridad asignados.

Artículo 9. *Organización y funcionamiento del Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Ministerio de Trabajo y Economía Social.*

1. El COSTIC se reunirá con carácter ordinario una vez al año y con carácter extraordinario cuando su presidente así lo convoque.

2. El COSTIC se podrá constituir, convocar, celebrar sus reuniones, adoptar acuerdos y remitir actas, tanto de forma presencial como a distancia, de conformidad con los artículos 17 y 18 de la Ley 40/2015, de 1 de octubre.

3. La Secretaría del COSTIC levantará acta de las reuniones, siendo enviadas a la Presidencia de dicho comité para su aprobación, en su caso, en el pleno siguiente. Esta Secretaría realizará, junto con la persona responsable de la seguridad del Departamento, todos los trabajos previos necesarios para las reuniones del COSTIC, apoyándose cuando lo requiera en las unidades y organismos del Departamento.

Corresponde a la Secretaría del COSTIC la revisión de la Política de Seguridad, al menos anualmente, proponiendo mejoras de esta y presentándola para su toma en consideración por parte del COSTIC, así como la actualización del marco normativo aplicable y la revisión de las normas de seguridad con la ayuda de las personas responsables de seguridad.

4. El COSTIC se regirá por esta orden y por las normas previstas para los órganos colegiados en la sección 3.ª del capítulo II del título preliminar de la Ley 40/2015, de 1 de octubre.

Artículo 10. *La persona responsable del sistema.*

1. La persona responsable del sistema es quien tiene la responsabilidad de desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida.

2. Son funciones de la persona responsable del sistema:

a) Definir la tipología y sistema de gestión del sistema de información estableciendo los criterios de uso y los servicios disponibles en el mismo.

b) Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.

c) Proponer la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser adoptada por las personas responsables de la información afectada o del servicio afectado y la persona responsable de la seguridad.

d) Para las demás funciones que por su naturaleza así lo requieran, se coordinará con la Secretaría General Técnica; en particular, en lo relativo a las actuaciones de implementación, desarrollo y administración del Archivo Electrónico Único del Departamento.

3. La persona titular de la Subdirección General de Tecnologías de la Información y Comunicaciones actuará como responsable del sistema en el ámbito del Departamento. Cada uno de los organismos públicos adscritos al Ministerio, a los que sea de aplicación esta política de seguridad, designarán una persona o unidad responsable del sistema.

Artículo 11. *Las personas o unidades administrativas responsables de la información.*

1. Conforme a los artículos 13 y 41 del Real Decreto 311/2022, de 3 de mayo, es responsable de la información la persona o unidad administrativa que tiene la potestad de establecer los requisitos de la información tratada y su implicación en la valoración del sistema de información del que forme parte.

2. Serán funciones de la persona responsable de la información, dentro de su ámbito de actuación, las siguientes:

a) Establecer los requisitos de la información tratada.

b) Valorar el impacto que tendría un incidente que afectase a la seguridad de la información con perjuicio para la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad.

La valoración de las consecuencias de un impacto negativo sobre la seguridad de la información se efectuará atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio y el respeto de la legalidad y de los derechos de los ciudadanos.

c) Aceptar los riesgos residuales respecto de la información, calculados en el análisis de riesgos.

d) Adoptar, de acuerdo con las personas responsables del servicio afectado y de seguridad, la decisión de la suspensión del manejo de una cierta información a propuesta de la persona responsable del sistema cuando haya sigo informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos.

3. La designación de la persona responsable de la información corresponderá a la persona titular de cada órgano superior o directivo dependiente del Ministerio y de cada uno de sus organismos públicos adscritos, a los que sea de aplicación esta política de seguridad, de acuerdo con su propia organización interna.

Artículo 12. *Las personas o unidades administrativas responsables de los servicios.*

1. Conforme a los artículos 13 y 41 Real Decreto 311/2022, de 3 de mayo, es responsable del servicio la persona o unidad administrativa, que tiene la potestad de establecer los requisitos del servicio prestado y su implicación en la valoración del nivel de seguridad de dicho servicio.

2. Serán funciones de la persona responsable del servicio, dentro de su ámbito de actuación las siguientes:

a) Determinar los requisitos de los servicios prestados.

b) Valorar el impacto que tendría un incidente que afectase a la seguridad de los servicios con perjuicio para la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad.

La valoración de las consecuencias de un impacto negativo sobre la seguridad de los servicios se efectuará atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los ciudadanos.

c) Aceptar los riesgos residuales respecto de los servicios, calculados en el análisis de riesgos.

d) Adoptar, de acuerdo con las personas responsables de la información y de seguridad, la decisión de la suspensión de la prestación de un cierto servicio a propuesta de la persona responsable del sistema cuando haya sigo informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos.

3. La designación de la persona responsable del servicio corresponderá a la persona titular de cada órgano superior o directivo dependiente del Ministerio y de cada uno de sus

organismos públicos adscritos, a los que sea de aplicación esta política de seguridad, de acuerdo con su propia organización interna.

4. La persona responsable de la información y la responsable del servicio podrán coincidir en una misma persona o unidad administrativa.

Artículo 13. *La persona responsable de la seguridad.*

1. Conforme al artículo 13 del Real Decreto 311/2022, de 3 de mayo, la persona responsable de seguridad es la persona que determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, y supervisa la implantación de las medidas necesarias para garantizar que se satisfacen dichos requisitos y reportar sobre estas cuestiones.

2. Serán funciones de la persona responsable de seguridad, dentro de su ámbito de actuación, las siguientes:

a) Mantener y verificar el nivel adecuado de seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información.

b) Promover la formación y concienciación en materia de seguridad de la información.

c) Designar responsables de la ejecución del análisis de riesgos y de la declaración de aplicabilidad, identificar medidas de seguridad, determinar las configuraciones necesarias y elaborar la documentación del sistema.

d) Determinar la categoría de seguridad del sistema en colaboración con la persona responsable del sistema y con las responsables de la información y del servicio.

e) Participar en la elaboración e implantación de los planes de mejora de la seguridad y, en su caso, en la de los planes de continuidad, procediendo a su validación.

f) Gestionar y asegurar las revisiones externas o internas del sistema, incluyendo auditorías que serán transmitidas a las personas responsables de los sistemas de información para el seguimiento y resolución de las deficiencias encontradas.

g) Gestionar los procesos de certificación y las declaraciones de aplicabilidad pertinentes de los sistemas de información.

h) Generar y mantener actualizada la documentación relativa a su ámbito de responsabilidad.

i) Adoptar, de acuerdo con las personas responsables de la información y del servicio afectado, la decisión de la suspensión del manejo de una cierta información o la prestación de un cierto servicio a propuesta de la persona responsable del sistema cuando haya sido informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos.

3. La persona titular de la Subsecretaría designará a la persona responsable de seguridad del Ministerio. Asimismo, designará al responsable de seguridad de cada organismo público adscrito al Departamento, a propuesta del organismo correspondiente.

De acuerdo con lo previsto en el artículo 13.3 del Real Decreto 311/2022, de 3 de mayo, la persona responsable de la seguridad será distinta de la responsable del sistema, no debiendo existir dependencia jerárquica entre ambas. En aquellas situaciones excepcionales en las que la ausencia justificada de recursos haga necesario que ambas funciones recaigan en la misma persona o en distintas personas entre las que exista relación jerárquica, deberán aplicarse medidas compensatorias para garantizar la finalidad del principio de diferenciación de responsabilidades previsto en el artículo 11 del citado real decreto.

Cuando la complejidad, distribución, separación física de sus elementos o número de usuarios de los sistemas de información lo justifiquen, la persona titular de la Subsecretaría podrá designar a las personas responsables de seguridad delegadas que considere necesarias, que tendrán dependencia funcional directa de la persona responsable de seguridad del Ministerio y que serán responsables, en su ámbito, de todas aquellas acciones que aquella les delegue.

Para garantizar que la persona responsable de seguridad no reciba instrucciones que limiten el desempeño de sus funciones, las desempeñará con independencia de las unidades que gestionen las tecnologías de la información y comunicaciones, y en estas funciones dependerá de la Presidencia del COSTIC.

Artículo 14. *Delegado de protección de datos.*

El delegado de protección de datos tiene carácter asesor y supervisor para el cumplimiento de lo dispuesto en el RGPD y demás normativa aplicable sobre protección de datos personales, debiéndose garantizar su independencia dentro de la organización y evitar cualquier conflicto de intereses, así como proveer de los medios necesarios para el desarrollo de sus funciones conforme al artículo 39 del RGPD.

El asesoramiento y supervisión del delegado de protección de datos se extiende a aquellas medidas de seguridad que se quieran implementar con finalidades distintas a garantizar la protección de datos, en la medida que impliquen un tratamiento adicional de datos personales.

Dentro de la gestión general de incidentes, el delegado de protección de datos intervendrá en la gestión de las brechas de datos personales, principalmente en su posición de interlocutor de la persona responsable o encargada del tratamiento ante la Agencia Española de Protección de Datos.

Artículo 15. *Tratamiento de datos personales.*

1. Se aplicarán a los datos de carácter personal que sean objeto de tratamiento por parte del Ministerio de Trabajo y Economía Social las medidas de seguridad apropiadas derivadas del análisis de riesgos de privacidad, así como de la evaluación de impacto relativa a la protección de datos, tal y como se detalla en el artículo 32 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.

Cuando un sistema de información trate datos personales, la persona responsable o la encargada del tratamiento, asesoradas por la persona designada como delegada de protección de datos, realizarán un análisis de riesgos, conforme al artículo 24 del Reglamento General de Protección de Datos.

La identificación de los riesgos específicos para los derechos y libertades de las personas físicas en relación con los tratamientos efectuados por la entidad debe ser previo al análisis de riesgos de sistemas donde se implementen los tratamientos, con el fin de permitir que el sistema de seguridad sea adecuado al riesgo que los tratamientos suponen para los derechos y libertades de las personas.

Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, la persona responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales, de conformidad con lo establecido en el artículo 35 del RGPD.

Además, en cumplimiento de la disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre, se aplicarán las medidas de seguridad que correspondan de las previstas en el ENS, para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del RGPD.

En el caso de que el análisis de riesgos y la evaluación de impacto en su caso, determine medidas agravadas respecto a la normativa recogida en el anexo II del Real Decreto 311/2022, de 3 de mayo, dichas medidas serán las que se implementarán en la protección de datos personales.

2. En función de las diversas situaciones que puedan producirse en materia de protección de datos personales, se establecerá la oportuna coordinación con la persona designada como delegada de protección de datos, de conformidad con el artículo 37 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 y el artículo 34 de la Ley Orgánica 3/2018 de 5 de diciembre, y, en la medida en que sea preciso, con las personas responsables y con las personas encargadas del tratamiento de datos personales.

Especialmente, se prestará apoyo a la persona designada como delegada de protección de datos, para la elaboración de propuestas o informes relativos a las reclamaciones de los interesados, comunicación de brechas de datos personales y respuestas a los requerimientos de la Agencia Española de Protección de Datos.

Artículo 16. *Normativa de seguridad.*

1. La normativa de seguridad del Ministerio de Trabajo y Economía Social se estructura en cuatro niveles siendo de obligada aplicación los tres primeros de la siguiente manera:

a) Primer nivel: La Política de Seguridad que queda regulada en esta orden ministerial.

b) Segundo nivel: Las normas de seguridad, instrucciones, protocolos, entre otros instrumentos, que concretan la Política de Seguridad y que deben especificar de forma concisa, transparente, inteligible y accesible, con un lenguaje claro y sencillo los objetivos de seguridad que se desean alcanzar.

c) Tercer nivel: Los procedimientos de seguridad, que se describen en los instrumentos referidos en el punto anterior, indican explícitamente y paso a paso cómo realizar una cierta actividad. Cada procedimiento debe detallar:

1.º En qué condiciones debe aplicarse.

2.º Quiénes son los que deben llevarlo a cabo.

3.º Qué es lo que hay que hacer en cada momento, incluyendo, en su caso, el registro de la actividad realizada.

4.º Cómo se miden sus resultados.

5.º Cómo se reportan posibles mejoras y deficiencias en los procedimientos.

d) Cuarto nivel: abarca la documentación de buenas prácticas, las recomendaciones formuladas y cualesquiera otros contenidos que afecten de manera no esencial a los conceptos constitutivos de los niveles anteriores.

Artículo 17. *Actuación y efectos respecto a la información correspondiente a otros entes o servicios de competencia ajena al Departamento.*

1. Cuando el Ministerio de Trabajo y Economía Social preste servicios a otros organismos o maneje información de otros organismos, se hará partícipes a los mismos de la política de seguridad. El Ministerio de Trabajo y Economía Social definirá y aprobará los canales para la coordinación de la información y los procedimientos de actuación para la reacción ante incidentes de seguridad, así como el resto de las actuaciones que el Departamento lleve a cabo en materia de seguridad en relación con otros organismos.

2. Cuando el Ministerio de Trabajo y Economía Social utilice servicios proporcionados por terceros o ceda información a terceros, se les hará partícipe de la política de seguridad y de la normativa de seguridad existente que atañe a dichos servicios o información. Estos sujetos que se relacionen con el Ministerio quedarán vinculados por las obligaciones establecidas en la mencionada normativa y podrán desarrollar sus propios procedimientos operativos para ejecutarlas. Se establecerán procedimientos específicos de comunicación y resolución de incidencias y se garantizará que su personal esté adecuadamente concienciado y formado en materia de seguridad.

3. Cuando algún aspecto de la política de seguridad no pueda ser satisfecho por una tercera parte según lo dispuesto en los párrafos anteriores, se requerirá un informe de la persona responsable de seguridad del Departamento u organismo adscrito al mismo, que precise los riesgos en los que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por las personas responsables de la información y de los servicios afectados antes de que la prestación de servicios o la cesión de la información continúen su ejecución.

4. Cuando la información contenga datos de carácter personal quedará sujeta a la normativa sobre protección de datos personales por la que están obligados a velar tanto las personas responsables como las encargadas del tratamiento.

Artículo 18. *Formación y concienciación.*

1. Todo el personal del Ministerio de Trabajo y Economía Social relacionado con la información, los servicios y los sistemas de información deberá conocer sus deberes y obligaciones en esta materia de seguridad de la información e identificar de forma inequívoca a las personas responsables de velar por su cumplimiento.

2. Para garantizar la seguridad de las tecnologías de la información aplicable a los sistemas y servicios del Ministerio de Trabajo y Economía Social, el COSTIC propondrá los mecanismos necesarios para desarrollar las actividades para la concienciación y la

formación específica necesaria e imprescindible, en materia de política de seguridad de la información, en todos los niveles de la organización.

Disposición adicional única. *No incremento del gasto público.*

Las medidas incluidas en esta orden no supondrán incremento del gasto, y serán atendidas con los medios personales, técnicos y presupuestarios asignados al Ministerio de Trabajo y Economía Social.

Disposición derogatoria única. *Derogación normativa.*

Quedan derogadas, en lo que afecta a las competencias del Ministerio de Trabajo y Economía Social, la Orden TIN/3016/2011, de 28 de octubre, por la que se crea el Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Ministerio de Trabajo e Inmigración, y la Orden del Ministerio de Empleo y Seguridad Social, de 30 de julio de 2012, por la que se aprueba la Política de Seguridad de los Sistemas de Información del Ministerio de Empleo y Seguridad Social.

Disposición final primera. *Instrucciones de aplicación.*

La persona titular de la Subsecretaría de Trabajo y Economía Social podrá dictar las instrucciones necesarias para el adecuado cumplimiento de esta orden.

Disposición final segunda. *Publicidad de la Política de Seguridad.*

Esta orden se publicará en el «Boletín Oficial del Estado» y en la sede electrónica del Ministerio de Trabajo y Economía Social.

Disposición final tercera. *Entrada en vigor.*

La presente orden entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

§ 10

Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica

Ministerio de la Presidencia
«BOE» núm. 25, de 29 de enero de 2010
Última modificación: 6 de noviembre de 2024
Referencia: BOE-A-2010-1331

I

La interoperabilidad es la capacidad de los sistemas de información y de los procedimientos a los que éstos dan soporte, de compartir datos y posibilitar el intercambio de información y conocimiento entre ellos. Resulta necesaria para la cooperación, el desarrollo, la integración y la prestación de servicios conjuntos por las Administraciones públicas; para la ejecución de las diversas políticas públicas; para la realización de diferentes principios y derechos; para la transferencia de tecnología y la reutilización de aplicaciones en beneficio de una mejor eficiencia; para la cooperación entre diferentes aplicaciones que habiliten nuevos servicios; todo ello facilitando el desarrollo de la administración electrónica y de la sociedad de la información.

En el ámbito de las Administraciones públicas, la consagración del derecho de los ciudadanos a comunicarse con ellas a través de medios electrónicos comporta una obligación correlativa de las mismas. Esta obligación tiene, como premisas, la promoción de las condiciones para que la libertad y la igualdad sean reales y efectivas, así como la remoción de los obstáculos que impidan o dificulten el ejercicio pleno del principio de neutralidad tecnológica y de adaptabilidad al progreso de las tecnologías de la información y las comunicaciones, garantizando con ello la independencia en la elección de las alternativas tecnológicas por los ciudadanos, así como la libertad de desarrollar e implantar los avances tecnológicos en un ámbito de libre mercado.

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, reconoce el protagonismo de la interoperabilidad y se refiere a ella como uno de los aspectos en los que es obligado que las previsiones normativas sean comunes y debe ser, por tanto, abordado por la regulación del Estado. La interoperabilidad se recoge dentro del principio de cooperación en el artículo 4 y tiene un protagonismo singular en el título cuarto dedicado a la Cooperación entre Administraciones para el impulso de la administración electrónica. En dicho título el aseguramiento de la interoperabilidad de los sistemas y aplicaciones empleados por las Administraciones públicas figura en el artículo 40 entre las funciones del órgano de cooperación en esta materia, el Comité Sectorial de Administración Electrónica. A continuación, el artículo 41 se refiere a la aplicación por parte de las Administraciones públicas de las medidas informáticas, tecnológicas y organizativas, y de

seguridad, que garanticen un adecuado nivel de interoperabilidad técnica, semántica y organizativa y eviten discriminación a los ciudadanos por razón de su elección tecnológica. Y, seguidamente, el artículo 42.1 crea el Esquema Nacional de Interoperabilidad que comprenderá el conjunto de criterios y recomendaciones en materia de seguridad, conservación y normalización que deberán ser tenidos en cuenta por las Administraciones públicas para la toma de decisiones tecnológicas que garanticen la interoperabilidad, entre éstas y con los ciudadanos.

La finalidad del Esquema Nacional de Interoperabilidad es la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones públicas, que permita el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunda en beneficio de la eficacia y la eficiencia.

II

El Esquema Nacional de Interoperabilidad tiene presentes las recomendaciones de la Unión Europea, la situación tecnológica de las diferentes Administraciones públicas, así como los servicios electrónicos existentes en las mismas, la utilización de estándares abiertos, así como en su caso y, de forma complementaria, estándares de uso generalizado por los ciudadanos.

Su articulación se ha realizado atendiendo a la normativa nacional sobre acceso electrónico de los ciudadanos a los servicios públicos, protección de datos de carácter personal, firma electrónica y documento nacional de identidad electrónico, accesibilidad, uso de lenguas oficiales, reutilización de la información en el sector público y órganos colegiados responsables de la administración electrónica. Se han tenido en cuenta otros instrumentos, tales como el Esquema Nacional de Seguridad, desarrollado al amparo de lo dispuesto en la Ley 11/2007, de 22 de junio, o antecedentes como los Criterios de Seguridad, Normalización y Conservación de las aplicaciones utilizadas para el ejercicio de potestades.

En términos de las recomendaciones de la Unión Europea se atiende al Marco Europeo de Interoperabilidad, elaborado por el programa comunitario IDABC, así como a otros instrumentos y actuaciones elaborados por este programa y que inciden en alguno de los múltiples aspectos de la interoperabilidad, tales como el Centro Europeo de Interoperabilidad Semántica, el Observatorio y Repositorio de Software de Fuentes Abiertas y la Licencia Pública de la Unión Europea. También se atiende a la Decisión 922/2009 del Parlamento Europeo y del Consejo, de 16 de septiembre de 2009, relativa a las soluciones de interoperabilidad para las administraciones públicas europeas, a los planes de acción sobre administración electrónica en materia de interoperabilidad y de aspectos relacionados, particularmente, con la política comunitaria de compartir, reutilizar y colaborar.

III

Este real decreto se limita a establecer los criterios y recomendaciones, junto con los principios específicos necesarios, que permitan y favorezcan el desarrollo de la interoperabilidad en las Administraciones públicas desde una perspectiva global y no fragmentaria, de acuerdo con el interés general, naturaleza y complejidad de la materia regulada, en el ámbito de la Ley 11/2007, de 22 de junio, al objeto de conseguir un común denominador normativo.

En consecuencia, el Esquema Nacional de Interoperabilidad atiende a todos aquellos aspectos que conforman de manera global la interoperabilidad. En primer lugar, se atiende a las dimensiones organizativa, semántica y técnica a las que se refiere el artículo 41 de la Ley 11/2007, de 22 de junio; en segundo lugar, se tratan los estándares, que la Ley 11/2007, de 22 de junio, pone al servicio de la interoperabilidad así como de la independencia en la elección de las alternativas tecnológicas y del derecho de los ciudadanos a elegir las aplicaciones o sistemas para relacionarse con las Administraciones públicas; en tercer lugar, se tratan las infraestructuras y los servicios comunes, elementos reconocidos de dinamización, simplificación y propagación de la interoperabilidad, a la vez que facilitadores de la relación multilateral; en cuarto lugar, se trata la reutilización, aplicada a las aplicaciones

de las Administraciones públicas, de la documentación asociada y de otros objetos de información, dado que la voz «compartir» se encuentra presente en la definición de interoperabilidad recogida en la Ley 11/2007, de 22 de junio, y junto con «reutilizar», ambas son relevantes para la interoperabilidad y se encuentran entroncadas con las políticas de la Unión Europea en relación con la idea de compartir, reutilizar y colaborar; en quinto lugar, se trata la interoperabilidad de la firma electrónica y de los certificados; por último, se atiende a la conservación, según lo establecido en la citada Ley 11/2007,de 22 de junio, como manifestación de la interoperabilidad a lo largo del tiempo, y que afecta de forma singular al documento electrónico.

En esta norma se hace referencia a la interoperabilidad como un proceso integral, en el que no caben actuaciones puntuales o tratamientos coyunturales, debido a que la debilidad de un sistema la determina su punto más frágil y, a menudo, este punto es la coordinación entre medidas individualmente adecuadas pero deficientemente ensambladas.

La norma se estructura en doce capítulos, cuatro disposiciones adicionales, dos disposiciones transitorias, una disposición derogatoria, tres disposiciones finales y un anexo conteniendo el glosario de términos.

El Esquema Nacional de Interoperabilidad se remite al Esquema Nacional de Seguridad para las cuestiones relativas en materia de seguridad que vayan más allá de los aspectos necesarios para garantizar la interoperabilidad.

El presente real decreto se aprueba en aplicación de lo dispuesto en la disposición final octava de la Ley 11/2007, de 22 de junio y, de acuerdo con lo dispuesto en el artículo 42, apartado 3, y disposición final primera de dicha norma, se ha elaborado con la participación de todas las Administraciones Públicas a las que les es de aplicación, ha sido informado favorablemente por la Comisión Permanente del Consejo Superior de Administración Electrónica, la Conferencia Sectorial de Administración Pública y la Comisión Nacional de Administración Local; y ha sido sometido al previo informe de la Agencia Española de Protección de Datos. Asimismo se ha sometido a la audiencia de los ciudadanos según las previsiones establecidas en el artículo 24 de la Ley 50/1997, de 27 de noviembre, del Gobierno.

En su virtud, a propuesta de la Ministra de la Presidencia, de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros en su reunión del día 8 de enero de 2010,

DISPONGO:

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

1. El presente real decreto tiene por objeto regular el Esquema Nacional de Interoperabilidad establecido en el artículo 42 de la Ley 11/2007, de 22 de junio.

2. El Esquema Nacional de Interoperabilidad comprenderá los criterios y recomendaciones de seguridad, normalización y conservación de la información, de los formatos y de las aplicaciones que deberán ser tenidos en cuenta por las Administraciones públicas para asegurar un adecuado nivel de interoperabilidad organizativa, semántica y técnica de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias y para evitar la discriminación a los ciudadanos por razón de su elección tecnológica.

Artículo 2. *Definiciones.*

A los efectos previstos en este real decreto, las definiciones, palabras, expresiones y términos se entenderán en el sentido indicado en el Glosario de Términos incluido en el anexo.

Artículo 3. *Ámbito de aplicación.*

1. El ámbito de aplicación del presente real decreto será el establecido en el artículo 2 de la Ley 11/2007, de 22 de junio.
2. El Esquema Nacional de Interoperabilidad y sus normas de desarrollo, prevalecerán sobre cualquier otro criterio en materia de política de interoperabilidad en la utilización de medios electrónicos para el acceso de los ciudadanos a los servicios públicos.

CAPÍTULO II

Principios básicos

Artículo 4. *Principios básicos del Esquema Nacional de Interoperabilidad.*

La aplicación del Esquema Nacional de Interoperabilidad se desarrollará de acuerdo con los principios generales establecidos en el artículo 4 de la Ley 11/2007, de 22 de junio, y con los siguientes principios específicos de la interoperabilidad:

a) La interoperabilidad como cualidad integral.
b) Carácter multidimensional de la interoperabilidad.
c) Enfoque de soluciones multilaterales.

Artículo 5. *La interoperabilidad como cualidad integral.*

La interoperabilidad se tendrá presente de forma integral desde la concepción de los servicios y sistemas y a lo largo de su ciclo de vida: planificación, diseño, adquisición, construcción, despliegue, explotación, publicación, conservación y acceso o interconexión con los mismos.

Artículo 6. *Carácter multidimensional de la interoperabilidad.*

La interoperabilidad se entenderá contemplando sus dimensiones organizativa, semántica y técnica. La cadena de interoperabilidad se manifiesta en la práctica en los acuerdos interadministrativos, en el despliegue de los sistemas y servicios, en la determinación y uso de estándares, en las infraestructuras y servicios básicos de las Administraciones públicas y en la publicación y reutilización de las aplicaciones de las Administraciones públicas, de la documentación asociada y de otros objetos de información. Todo ello sin olvidar la dimensión temporal que ha de garantizar el acceso a la información a lo largo del tiempo.

Artículo 7. *Enfoque de soluciones multilaterales.*

Se favorecerá la aproximación multilateral a la interoperabilidad de forma que se puedan obtener las ventajas derivadas del escalado, de la aplicación de las arquitecturas modulares y multiplataforma, de compartir, de reutilizar y de colaborar.

CAPÍTULO III

Interoperabilidad organizativa

Artículo 8. *Servicios de las Administraciones públicas disponibles por medios electrónicos.*

1. Las Administraciones públicas establecerán y publicarán las condiciones de acceso y utilización de los servicios, datos y documentos en formato electrónico que pongan a disposición del resto de Administraciones especificando las finalidades, las modalidades de consumo, consulta o interacción, los requisitos que deben satisfacer los posibles usuarios de los mismos, los perfiles de los participantes implicados en la utilización de los servicios, los protocolos y criterios funcionales o técnicos necesarios para acceder a dichos servicios, los necesarios mecanismos de gobierno de los sistemas interoperables, así como las condiciones de seguridad aplicables. Estas condiciones deberán en todo caso resultar conformes a los principios, derechos y obligaciones contenidos en la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de

desarrollo, así como a lo dispuesto en el Esquema Nacional de Seguridad, y los instrumentos jurídicos que deberán suscribir las Administraciones públicas requeridoras de dichos servicios, datos y documentos.

Se potenciará el establecimiento de convenios entre las Administraciones públicas emisoras y receptoras y, en particular, con los nodos de interoperabilidad previstos en el apartado 3 de este artículo, con el objetivo de simplificar la complejidad organizativa sin menoscabo de las garantías jurídicas.

Al objeto de dar cumplimiento de manera eficaz a lo establecido en el artículo 9 de la Ley 11/2007, de 22 de junio, en el Comité Sectorial de Administración electrónica se identificarán, catalogarán y priorizarán los servicios de interoperabilidad que deberán prestar las diferentes Administraciones públicas.

2. Las Administraciones públicas publicarán aquellos servicios que pongan a disposición de las demás administraciones a través de la Red de comunicaciones de las Administraciones públicas españolas, o de cualquier otra red equivalente o conectada a la misma que garantice el acceso seguro al resto de administraciones.

3. Las Administraciones públicas podrán utilizar nodos de interoperabilidad, entendidos como entidades a las cuales se les encomienda la gestión de apartados globales o parciales de la interoperabilidad organizativa, semántica o técnica.

Artículo 9. *Inventarios de información administrativa.*

1. Cada Administración Pública mantendrá actualizado el conjunto de sus inventarios de información administrativa que incluirá, al menos:

a) La relación de los procedimientos administrativos y servicios prestados de forma clasificada y estructurada. Las Administraciones Públicas conectarán electrónicamente sus inventarios con el Sistema de Información Administrativa gestionado por el Ministerio de Política Territorial y Función Pública en colaboración con el Ministerio de Asuntos Económicos y Transformación Digital.

b) La relación de sus órganos administrativos y oficinas orientadas al público y sus relaciones entre ellos. Dicho inventario se conectará electrónicamente con el Directorio Común de Unidades Orgánicas y Oficinas, gestionado por el Ministerio de Asuntos Económicos y Transformación Digital, en colaboración con el Ministerio de Política Territorial y Función Pública, que proveerá una codificación unívoca.

2. Cada Administración Pública regulará la creación y mantenimiento de estos dos inventarios, en las condiciones que se determinen, con carácter general, por las normas técnicas de interoperabilidad correspondientes; en su caso, las Administraciones Públicas podrán hacer uso de los citados Sistema de Información Administrativa y Directorio Común de Unidades Orgánicas y Oficinas para la creación y mantenimiento de sus propios inventarios. Para la descripción y modelización de los procedimientos administrativos y de los procesos que los soportan será de aplicación lo previsto sobre estándares en el artículo 11.

CAPÍTULO IV

Interoperabilidad semántica

Artículo 10. *Activos semánticos.*

1. Se establecerá y mantendrá actualizada la Relación de modelos de datos de intercambio que tengan el carácter de comunes, que serán de preferente aplicación para los intercambios de información en las Administraciones públicas, de acuerdo con el procedimiento establecido en disposición adicional primera.

2. Los órganos de la Administración pública o Entidades de Derecho Público vinculadas o dependientes de aquélla, titulares de competencias en materias sujetas a intercambio de información con los ciudadanos y con otras Administraciones públicas, así como en materia de infraestructuras, servicios y herramientas comunes, establecerán y publicarán los correspondientes modelos de datos de intercambio que serán de obligatoria aplicación para los intercambios de información en las Administraciones públicas.

3. Los modelos de datos a los que se refieren los apartados 1 y 2, se ajustarán a lo previsto sobre estándares en el artículo 11 y se publicarán, junto con las definiciones y codificaciones asociadas, a través del Centro de Interoperabilidad Semántica de la Administración, según las condiciones de licenciamiento previstas en el artículo 16.

4. Las definiciones y codificaciones empleadas en los modelos de datos a los que se refieren los apartados anteriores tendrán en cuenta lo dispuesto en la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública y el resto de disposiciones que regulan la función estadística.

CAPÍTULO V

Interoperabilidad técnica

Artículo 11. *Estándares aplicables.*

1. Las Administraciones públicas usarán estándares abiertos, así como, en su caso y de forma complementaria, estándares que sean de uso generalizado por los ciudadanos, al objeto de garantizar la independencia en la elección de alternativas tecnológicas por los ciudadanos y las Administraciones públicas y la adaptabilidad al progreso de la tecnología y, de forma que:

a) Los documentos y servicios de administración electrónica que los órganos o Entidades de Derecho Público emisores pongan a disposición de los ciudadanos o de otras Administraciones públicas se encontrarán, como mínimo, disponibles mediante estándares abiertos.

b) Los documentos, servicios electrónicos y aplicaciones puestos por las Administraciones públicas a disposición de los ciudadanos o de otras Administraciones públicas serán, según corresponda, visualizables, accesibles y funcionalmente operables en condiciones que permitan satisfacer el principio de neutralidad tecnológica y eviten la discriminación a los ciudadanos por razón de su elección tecnológica.

2. En las relaciones con los ciudadanos y con otras Administraciones públicas, el uso en exclusiva de un estándar no abierto sin que se ofrezca una alternativa basada en un estándar abierto se limitará a aquellas circunstancias en las que no se disponga de un estándar abierto que satisfaga la funcionalidad satisfecha por el estándar no abierto en cuestión y sólo mientras dicha disponibilidad no se produzca. Las Administraciones públicas promoverán las actividades de normalización con el fin de facilitar la disponibilidad de los estándares abiertos relevantes para sus necesidades.

3. Para la selección de estándares, en general y, para el establecimiento del catálogo de estándares, en particular, se atenderá a los siguientes criterios:

a) El uso de las especificaciones técnicas de las TIC en la contratación pública junto con las definiciones de norma y especificación técnica establecidos en el Reglamento n.º 1025/2012, del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, sobre normalización europea.

b) La definición de estándar abierto establecida en la Ley 11/2007, de 22 de junio, anexo, letra k).

c) Carácter de especificación formalizada.

d) Definición de «coste que no suponga una dificultad de acceso», establecida en el anexo de este real decreto.

e) Consideraciones adicionales referidas a la adecuación del estándar a las necesidades y funcionalidad requeridas; a las condiciones relativas a su desarrollo, uso o implementación, documentación disponible y completa, publicación, y gobernanza del estándar; a las condiciones relativas a la madurez, apoyo y adopción del mismo por parte del mercado, a su potencial de reutilización, a la aplicabilidad multiplataforma y multicanal y a su implementación bajo diversos modelos de desarrollo de aplicaciones.

4. Para el uso de los estándares complementarios a la selección indicada en el apartado anterior, se tendrá en cuenta la definición de «uso generalizado por los ciudadanos» establecida en el anexo del presente real decreto.

5. En cualquier caso los ciudadanos podrán elegir las aplicaciones o sistemas para relacionarse con las Administraciones públicas, o dirigirse a las mismas, siempre y cuando utilicen estándares abiertos o, en su caso, aquellos otros que sean de uso generalizado por los ciudadanos. Para facilitar la interoperabilidad con las Administraciones públicas el catálogo de estándares contendrá una relación de estándares abiertos y en su caso complementarios aplicables.

CAPÍTULO VI

Infraestructuras y servicios comunes

Artículo 12. *Uso de infraestructuras y servicios comunes y herramientas genéricas.*

Las Administraciones públicas enlazarán aquellas infraestructuras y servicios que puedan implantar en su ámbito de actuación con las infraestructuras y servicios comunes que proporcione la Administración General del Estado para facilitar la interoperabilidad y la relación multilateral en el intercambio de información y de servicios entre todas las Administraciones públicas.

CAPÍTULO VII

Comunicaciones de las Administraciones públicas

Artículo 13. *Red de comunicaciones de las Administraciones públicas españolas.*

1. Al objeto de satisfacer lo previsto en el artículo 43 de la Ley 11/2007, de 22 de junio, las Administraciones públicas utilizarán preferentemente la Red de comunicaciones de las Administraciones públicas españolas para comunicarse entre sí, para lo cual conectarán a la misma, bien sus respectivas redes, bien sus nodos de interoperabilidad, de forma que se facilite el intercambio de información y de servicios entre las mismas, así como la interconexión con las redes de las Instituciones de la Unión Europea y de otros Estados miembros.

La Red SARA prestará la citada Red de comunicaciones de las Administraciones públicas españolas.

2. Para la conexión a la Red de comunicaciones de las Administraciones públicas españolas serán de aplicación los requisitos previstos en la disposición adicional primera.

Artículo 14. *Plan de direccionamiento de la Administración.*

Las Administraciones Públicas aplicarán el Plan de direccionamiento e interconexión de redes en la Administración, desarrollado en la norma técnica de interoperabilidad correspondiente, para su interconexión a través de las redes de comunicaciones.

Artículo 15. *Hora oficial.*

1. Los sistemas o aplicaciones implicados en la provisión de un servicio público por vía electrónica se sincronizarán con la hora oficial, con una precisión y desfase que garanticen la certidumbre de los plazos establecidos en el trámite administrativo que satisfacen.

2. La sincronización de la fecha y la hora se realizará con el Real Instituto y Observatorio de la Armada, de conformidad con lo previsto sobre la hora legal en el Real Decreto 1308/1992, de 23 de octubre, por el que se declara al Laboratorio del Real Instituto y Observatorio de la Armada, como laboratorio depositario del patrón nacional de Tiempo y laboratorio asociado al Centro Español de Metrología y, cuando sea posible, con la hora oficial a nivel europeo.

CAPÍTULO VIII

Reutilización y transferencia de tecnología

Artículo 16. *Condiciones de licenciamiento aplicables.*

1. Las condiciones de licenciamiento de las aplicaciones informáticas, documentación asociada, y cualquier otro objeto de información cuya titularidad de los derechos de la propiedad intelectual sea de una Administración Pública y permita su puesta a disposición de otra Administración y de los ciudadanos tendrán en cuenta los siguientes aspectos:

a) El fin perseguido es el aprovechamiento y la reutilización de recursos públicos.
b) La completa protección contra su apropiación exclusiva o parcial por parte de terceros.
c) La exención de responsabilidad del cedente por el posible mal uso por parte del cesionario.
d) La no obligación de asistencia técnica o de mantenimiento por parte del cedente.
e) La ausencia total de responsabilidad por parte del cedente con respecto al cesionario en caso de errores o mal funcionamiento de la aplicación.
f) El licenciamiento se realizará por defecto sin contraprestación y sin necesidad de establecer convenio alguno. Sólo se podrá acordar la repercusión parcial del coste de adquisición o desarrollo de las aplicaciones cedidas en aquellos casos en los que este pago repercuta directamente en el incremento de funcionalidades del activo cedido, incluya adaptaciones concretas para su uso en el organismo cesionario, o impliquen el suministro de servicios de asistencia o soporte para su reutilización en el organismo cesionario.

2. Las Administraciones Públicas utilizarán para las aplicaciones informáticas, documentación asociada, y cualquier otro objeto de información declarados como de fuentes abiertas aquellas licencias que aseguren que los programas, datos o información cumplen los siguientes requisitos:

a) Pueden ejecutarse para cualquier propósito.
b) Permiten conocer su código fuente.
c) Pueden modificarse o mejorarse.
d) Pueden redistribuirse a otros usuarios con o sin cambios siempre que la obra derivada mantenga estas cuatro garantías.

3. Para este fin se procurará la aplicación de la Licencia Pública de la Unión Europea, sin perjuicio de otras licencias que garanticen los mismos derechos expuestos en los apartados 1 y 2.
4. A efectos de facilitar el establecimiento de las condiciones de licenciamiento, las Administraciones Públicas incluirán en los pliegos de cláusulas técnicas de aquellos contratos que tengan por finalidad el desarrollo de nuevas aplicaciones informáticas, los siguientes aspectos:

a) Que la Administración contratante adquiera los derechos completos de propiedad intelectual de las aplicaciones y cualquier otro objeto de información que se desarrollen como objeto de ese contrato.
b) Que en el caso de reutilizar activos previamente existentes, la Administración contratante reciba un producto que pueda ofrecer para su reutilización posterior a otras Administraciones Públicas. Además, en el caso de partir de productos de fuentes abiertas, que sea posible declarar como de fuentes abiertas la futura aplicación desarrollada.

Artículo 17. *Directorios de aplicaciones reutilizables.*

1. La Administración General del Estado mantendrá el Directorio general de aplicaciones para su libre reutilización, de acuerdo al artículo 158 de la Ley 40/2015, de 1 octubre, a través del Centro de Transferencia de Tecnología. Este directorio podrá ser utilizado por otras Administraciones Públicas. En el caso de disponer de un directorio propio, deberá garantizar que las aplicaciones disponibles en ese directorio propio se pueden consultar también a través del Centro de Transferencia de Tecnología.
2. Las Administraciones Públicas conectarán los directorios de aplicaciones para su libre reutilización entre sí; y con instrumentos equivalentes del ámbito de la Unión Europea.

3. Las Administraciones Públicas publicarán las aplicaciones reutilizables, en modo producto o en modo servicio, en los directorios de aplicaciones para su libre reutilización, con al menos el siguiente contenido:

a) Código fuente de las aplicaciones finalizadas, en el caso de ser reutilizables en modo producto y haber sido declaradas de fuentes abiertas.
b) Documentación asociada.
c) Condiciones de licenciamiento de todos los activos, en el caso de ser reutilizables en modo producto, o nivel de servicio ofrecido, en el caso de ser reutilizables en modo servicio.
d) Los costes asociados a su reutilización, en el caso de que existieran.

4. Las Administraciones procurarán la incorporación a la aplicación original de aquellas modificaciones o adaptaciones realizadas sobre cualquier aplicación que se haya obtenido desde un directorio de aplicaciones reutilizables.

CAPÍTULO IX

Firma electrónica y certificados

Artículo 18. *Interoperabilidad en la política de firma electrónica y de certificados.*

1. La Administración General del Estado definirá una política de firma electrónica y de certificados que servirá de marco general de interoperabilidad para el reconocimiento mutuo de las firmas electrónicas basadas en certificados de documentos administrativos en las Administraciones Públicas.

Todos los organismos y entidades de derecho público de la Administración General del Estado aplicarán la política de firma electrónica y de certificados a que se refiere el párrafo anterior. La no aplicación de dicha política deberá ser justificada por el órgano u organismo competente y autorizada por la Secretaría General de Administración Digital.

2. Las restantes Administraciones Públicas podrán acogerse a la política de firma electrónica y de certificados a que hace referencia el apartado anterior.

3. Sin perjuicio de lo expuesto en el apartado anterior, las Administraciones Públicas podrán aprobar otras políticas de firma electrónica dentro de sus respectivos ámbitos competenciales.

Las políticas de firma electrónica que aprueben las Administraciones Públicas partirán de la norma técnica establecida a tal efecto en la disposición adicional primera, de los estándares técnicos existentes, y deberán ser interoperables con la política marco de firma electrónica mencionada en el apartado 1, en particular, con sus ficheros de implementación. La Administración Pública proponente de una política de firma electrónica particular garantizará su interoperabilidad con la citada política marco de firma electrónica y con sus correspondientes ficheros de implementación según las condiciones establecidas en la norma técnica de interoperabilidad recogida a tal efecto en la disposición adicional primera.

4. Al objeto de garantizar la interoperabilidad de las firmas electrónicas emitidas conforme a las políticas establecidas, las políticas de firma electrónica que las Administraciones Públicas aprueben deberán ser comunicadas, junto con sus correspondientes ficheros de implementación, a la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital.

5. Las Administraciones Públicas receptoras de documentos electrónicos firmados, siempre que hayan admitido con anterioridad la política de firma del emisor, permitirán la validación de las firmas electrónicas según la política de firma indicada en la firma del documento electrónico.

6. Los perfiles comunes de los campos de los certificados definidos por la política de firma electrónica y de certificados posibilitarán la interoperabilidad entre las aplicaciones usuarias, de manera que tanto la identificación como la firma electrónica generada a partir de estos perfiles comunes puedan ser reconocidos por las aplicaciones de las distintas Administraciones Públicas sin ningún tipo de restricción técnica, semántica u organizativa.

7. Los procedimientos en los que se utilicen certificados de firma electrónica deberán atenerse a la política de firma electrónica y de certificados aplicable en su ámbito, particularmente en la aplicación de los datos obligatorios y opcionales, las reglas de creación

y validación de firma electrónica, los algoritmos a utilizar y longitudes de clave mínimas aplicables.

Artículo 19. *Aspectos de interoperabilidad relativos a los prestadores de servicios de certificación.*

(Suprimido)

Artículo 20. *Plataformas de validación de certificados electrónicos y de firma electrónica.*

1. Las plataformas de validación de certificados electrónicos y de firma electrónica proporcionarán servicios de confianza a las aplicaciones usuarias o consumidoras de los servicios de certificación y firma, proporcionando servicios de validación de los certificados y firmas generadas y admitidas en diversos ámbitos de las Administraciones públicas.
2. Proporcionarán, en un único punto de llamada, todos los elementos de confianza y de interoperabilidad organizativa, semántica y técnica necesarios para integrar los distintos certificados reconocidos y firmas que pueden encontrase en los dominios de dos administraciones diferentes.
3. Potenciarán la armonización técnica y la utilización común de formatos, estándares y políticas de firma electrónica y de certificados para las firmas electrónicas entre las aplicaciones usuarias, y de otros elementos de interoperabilidad relacionados con los certificados, tales como el análisis de los campos y extracción univoca de la información pertinente. En particular, se tendrán en cuenta los estándares europeos de las Organizaciones Europeas de Estandarización en el campo de las Tecnologías de Información y Comunicación aplicadas a la firma electrónica.
4. Incorporarán las listas de confianza de los certificados interoperables entre las distintas Administraciones públicas nacionales y europeas según el esquema operativo de gestión correspondiente de la lista de confianza.

CAPÍTULO X

Recuperación y conservación del documento electrónico

Artículo 21. *Condiciones para la recuperación y conservación de documentos.*

1. Las Administraciones públicas adoptarán las medidas organizativas y técnicas necesarias con el fin de garantizar la interoperabilidad en relación con la recuperación y conservación de los documentos electrónicos a lo largo de su ciclo de vida. Tales medidas incluirán:

a) La definición de una política de gestión de documentos en cuanto al tratamiento, de acuerdo con las normas y procedimientos específicos que se hayan de utilizar en la formación y gestión de los documentos y expedientes.
b) La inclusión en los expedientes de un índice electrónico firmado por el órgano o entidad actuante que garantice la integridad del expediente electrónico y permita su recuperación.
c) La identificación única e inequívoca de cada documento por medio de convenciones adecuadas, que permitan clasificarlo, recuperarlo y referirse al mismo con facilidad.
d) La asociación de los metadatos mínimos obligatorios y, en su caso, complementarios, asociados al documento electrónico, a lo largo de su ciclo de vida, e incorporación al esquema de metadatos.
e) La clasificación, de acuerdo con un plan de clasificación adaptado a las funciones, tanto generales como específicas, de cada una de las Administraciones públicas y de las Entidades de Derecho Público vinculadas o dependientes de aquéllas.
f) El período de conservación de los documentos, establecido por las comisiones calificadoras que correspondan, de acuerdo con la legislación en vigor, las normas administrativas y obligaciones jurídicas que resulten de aplicación en cada caso.
g) El acceso completo e inmediato a los documentos a través de métodos de consulta en línea que permitan la visualización de los documentos con todo el detalle de su contenido, la recuperación exhaustiva y pertinente de los documentos, la copia o descarga en línea en los

formatos originales y la impresión a papel de aquellos documentos que sean necesarios. El sistema permitirá la consulta durante todo el período de conservación al menos de la firma electrónica, incluido, en su caso, el sello de tiempo, y de los metadatos asociados al documento.

h) La adopción de medidas para asegurar la conservación de los documentos electrónicos a lo largo de su ciclo de vida, de acuerdo con lo previsto en el artículo 22, de forma que se pueda asegurar su recuperación de acuerdo con el plazo mínimo de conservación determinado por las normas administrativas y obligaciones jurídicas, se garantice su conservación a largo plazo, se asegure su valor probatorio y su fiabilidad como evidencia electrónica de las actividades y procedimientos, así como la transparencia, la memoria y la identificación de los órganos de las Administraciones públicas y de las Entidades de Derecho Público vinculadas o dependientes de aquéllas que ejercen la competencia sobre el documento o expediente.

i) La coordinación horizontal entre el responsable de gestión de documentos y los restantes servicios interesados en materia de archivos.

j) Transferencia, en su caso, de los expedientes entre los diferentes repositorios electrónicos a efectos de conservación, de acuerdo con lo establecido en la legislación en materia de Archivos, de manera que se pueda asegurar su conservación, y recuperación a medio y largo plazo.

k) Si el resultado del procedimiento de evaluación documental así lo establece, borrado de la información, o en su caso, destrucción física de los soportes, de acuerdo con la legislación que resulte de aplicación, dejando registro de su eliminación.

l) La formación tecnológica del personal responsable de la ejecución y del control de la gestión de documentos, como de su tratamiento y conservación en archivos o repositorios electrónicos.

m) La documentación de los procedimientos que garanticen la interoperabilidad a medio y largo plazo, así como las medidas de identificación, recuperación, control y tratamiento de los documentos electrónicos.

2. A los efectos de lo dispuesto en el apartado 1, las Administraciones públicas crearán repositorios electrónicos, complementarios y equivalentes en cuanto a su función a los archivos convencionales, destinados a cubrir el conjunto del ciclo de vida de los documentos electrónicos.

Artículo 22. *Seguridad.*

1. Para asegurar la conservación de los documentos electrónicos se aplicará lo previsto en el Esquema Nacional de Seguridad en cuanto al cumplimento de los principios básicos y de los requisitos mínimos de seguridad mediante la aplicación de las medidas de seguridad adecuadas a los medios y soportes en los que se almacenen los documentos, de acuerdo con la categorización de los sistemas.

2. Cuando los citados documentos electrónicos contengan datos de carácter personal les será de aplicación lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y normativa de desarrollo.

3. Estas medidas se aplicarán con el fin de garantizar la integridad, autenticidad, confidencialidad, disponibilidad, trazabilidad, calidad, protección, recuperación y conservación física y lógica de los documentos electrónicos, sus soportes y medios, y se realizarán atendiendo a los riesgos a los que puedan estar expuestos y a los plazos durante los cuales deban conservarse los documentos.

4. Los aspectos relativos a la firma electrónica en la conservación del documento electrónico se establecerán en la Política de firma electrónica y de certificados, y a través del uso de formatos de firma longeva que preserven la conservación de las firmas a lo largo del tiempo.

Cuando la firma y los certificados no puedan garantizar la autenticidad y la evidencia de los documentos electrónicos a lo largo del tiempo, éstas les sobrevendrán a través de su conservación y custodia en los repositorios y archivos electrónicos, así como de los metadatos de gestión de documentos y otros metadatos vinculados, de acuerdo con las características que se definirán en la Política de gestión de documentos.

Artículo 23. *Formatos de los documentos.*

1. Con el fin de garantizar la conservación, el documento se conservará en el formato en que haya sido elaborado, enviado o recibido, y preferentemente en un formato correspondiente a un estándar abierto que preserve a lo largo del tiempo la integridad del contenido del documento, de la firma electrónica y de los metadatos que lo acompañan.

2. La elección de formatos de documento electrónico normalizados y perdurables para asegurar la independencia de los datos de sus soportes se realizará de acuerdo con lo previsto en el artículo 11.

3. Cuando exista riesgo de obsolescencia del formato o bien deje de figurar entre los admitidos en el presente Esquema Nacional de Interoperabilidad, se aplicarán procedimientos normalizados de copiado auténtico de los documentos con cambio de formato, de etiquetado con información del formato utilizado y, en su caso, de las migraciones o conversiones de formatos.

Artículo 24. *Digitalización de documentos en soporte papel.*

1. La digitalización de documentos en soporte papel por parte de las Administraciones públicas se realizará de acuerdo con lo indicado en la norma técnica de interoperabilidad correspondiente en relación con los siguientes aspectos:

a) Formatos estándares de uso común para la digitalización de documentos en soporte papel y técnica de compresión empleada, de acuerdo con lo previsto en el artículo 11.

b) Nivel de resolución.

c) Garantía de imagen fiel e íntegra.

d) Metadatos mínimos obligatorios y complementarios, asociados al proceso de digitalización.

2. La gestión y conservación del documento electrónico digitalizado atenderá a la posible existencia del mismo en otro soporte.

CAPÍTULO XI

Normas de conformidad

Artículo 25. *Sedes y registros electrónicos.*

La interoperabilidad de las sedes y registros electrónicos, así como la del acceso electrónico de los ciudadanos a los servicios públicos, se regirán por lo establecido en el Esquema Nacional de Interoperabilidad.

Artículo 26. *Ciclo de vida de servicios y sistemas.*

La conformidad con el Esquema Nacional de Interoperabilidad se incluirá en el ciclo de vida de los servicios y sistemas, acompañada de los correspondientes procedimientos de control.

Artículo 27. *Mecanismo de control.*

Cada órgano o Entidad de Derecho Público establecerá sus mecanismos de control para garantizar, de forma efectiva, el cumplimiento del Esquema Nacional de Interoperabilidad.

Artículo 28. *Publicación de conformidad.*

Los órganos y Entidades de Derecho Público de las Administraciones públicas darán publicidad, en las correspondientes sedes electrónicas, a las declaraciones de conformidad y a otros posibles distintivos de interoperabilidad de los que sean acreedores, obtenidos respecto al cumplimiento del Esquema Nacional de Interoperabilidad.

CAPÍTULO XII

Actualización

Artículo 29. *Actualización permanente.*

El Esquema Nacional de Interoperabilidad se deberá mantener actualizado de manera permanente. Se desarrollará y perfeccionará a lo largo del tiempo, en paralelo al progreso de los servicios de Administración Electrónica, de la evolución tecnológica y a medida que vayan consolidándose las infraestructuras que le apoyan.

Disposición adicional primera. *Desarrollo del Esquema Nacional de Interoperabilidad.*

1. Se desarrollarán las siguientes normas técnicas de interoperabilidad que serán de obligado cumplimiento por parte de las Administraciones Públicas:

a) Norma Técnica de Catálogo de estándares: establecerá un conjunto de estándares que satisfagan lo previsto en el artículo 11 de forma estructurada y con indicación de los criterios de selección y ciclo de vida aplicados.

b) Norma Técnica de Documento electrónico: tratará los metadatos mínimos obligatorios, la asociación de los datos y metadatos de firma o de sellado de tiempo, así como otros metadatos complementarios asociados; y los formatos de documento.

c) Norma Técnica de Digitalización de documentos: tratará los formatos y estándares aplicables, los niveles de calidad, las condiciones técnicas y los metadatos asociados al proceso de digitalización.

d) Norma Técnica de Expediente electrónico: tratará de su estructura y formato, así como de las especificaciones de los servicios de remisión y puesta a disposición.

e) Norma Técnica de Política de firma electrónica y de certificados de la Administración: Tratará, entre otras cuestiones recogidas en su definición en el anexo, aquellas que afectan a la interoperabilidad incluyendo los formatos de firma, los algoritmos a utilizar y longitudes mínimas de las claves, las reglas de creación y validación de la firma electrónica, la gestión de las políticas de firma, el uso de las referencias temporales y de sello de tiempo, así como la normalización de la representación de la firma electrónica en pantalla y en papel para el ciudadano y en las relaciones entre las Administraciones Públicas.

f) Norma Técnica de Protocolos de intermediación de datos: tratará las especificaciones de los protocolos de intermediación de datos que faciliten la integración y reutilización de servicios en las Administraciones Públicas y que serán de aplicación para los prestadores y consumidores de tales servicios.

g) Norma Técnica de Relación de modelos de datos que tengan el carácter de comunes en la Administración y aquellos que se refieran a materias sujetas a intercambio de información con los ciudadanos y otras Administraciones.

h) Norma Técnica de Política de gestión de documentos electrónicos: incluirá directrices para la asignación de responsabilidades, tanto directivas como profesionales, y la definición de los programas, procesos y controles de gestión de documentos y administración de los repositorios electrónicos, y la documentación de los mismos, a desarrollar por las Administraciones Públicas y por los organismos públicos y entidades de derecho público vinculados o dependientes de aquéllas.

i) Norma Técnica de Requisitos de conexión a la Red de comunicaciones de las Administraciones Públicas españolas.

j) Norma Técnica de Procedimientos de copiado auténtico y conversión entre documentos electrónicos, así como desde papel u otros medios físicos a formatos electrónicos.

k) Norma Técnica de Modelo de Datos para el intercambio de asientos entre las Entidades Registrales: tratará de aspectos funcionales y técnicos para el intercambio de asientos registrales, gestión de errores y excepciones, gestión de anexos, requerimientos tecnológicos y transformaciones de formatos.

l) Norma Técnica de Reutilización de recursos de información: tratará de las normas comunes sobre la localización, descripción e identificación unívoca de los recursos de información puestos a disposición del público por medios electrónicos para su reutilización.

m) Norma Técnica de interoperabilidad de inventario y codificación de objetos administrativos: tratará las reglas relativas a la codificación de objetos administrativos, así como la conexión entre los inventarios correspondientes, incluyendo, por un lado, las unidades orgánicas y oficinas de la Administración, y, por otro lado, la información administrativa de procedimientos y servicios.

n) Norma Técnica de Interoperabilidad de Transferencia e Ingreso de documentos y expedientes electrónicos: tratará los requisitos y condiciones relativos a la transferencia de agrupaciones documentales en formato electrónico, documentos y expedientes electrónicos, junto con los metadatos asociados, entre sistemas de gestión de documentos electrónicos y sistemas de archivo electrónico.

ñ) Norma Técnica de Interoperabilidad de Valoración y Eliminación de documentos y expedientes electrónicos: tratará las condiciones y requisitos relativos a la valoración de los documentos y expedientes electrónicos para establecimiento de plazos de conservación, transferencia y acceso o, en su caso, eliminación total o parcial.

o) Norma Técnica de Interoperabilidad de preservación de documentación electrónica: tratará las condiciones y requisitos relativos a la conservación de los documentos electrónicos para garantizar su autenticidad, integridad, confidencialidad, disponibilidad y trazabilidad, así como la protección, recuperación y conservación física y lógica de los documentos y su contexto.

p) Norma Técnica de Interoperabilidad de tratamiento y preservación de bases de datos: tratará las condiciones y requisitos relativos a la conservación de las bases de datos para garantizar su autenticidad, integridad, confidencialidad, disponibilidad y trazabilidad, y permitiendo la protección, recuperación y conservación física y lógica de los datos y su contexto.

q) Norma Técnica de Interoperabilidad de Plan de Direccionamiento: tratará reglas aplicables a la asignación y requisitos de direccionamiento IP para garantizar la correcta administración de la Red de comunicaciones de las Administraciones Públicas españolas y evitar el uso de direcciones duplicadas.

r) Norma Técnica de Interoperabilidad de reutilización de activos en modo producto y en modo servicio: tratará los requisitos y condiciones para facilitar la reutilización de activos tanto en modo producto como en modo servicio por las Administraciones Públicas españolas.

s) Norma Técnica de Interoperabilidad del modelo de datos y condiciones de interoperabilidad de los registros de funcionarios habilitados: tratará los aspectos funcionales y técnicos para la plena interoperabilidad de los registros electrónicos de funcionarios habilitados pertenecientes a las Administraciones, así como la interconexión de estos a las sedes electrónicas.

t) Norma Técnica de Interoperabilidad del modelo de datos y condiciones de interoperabilidad de los registros electrónicos de apoderamientos: tratará los aspectos funcionales y técnicos para la plena interoperabilidad de los registros electrónicos de apoderamientos pertenecientes a las Administraciones, así como la interconexión de estos a las sedes electrónicas, A los registros mercantiles, de la propiedad, y a los protocolos notariales.

u) Norma Técnica de Interoperabilidad de Sistema de Referencia de documentos y repositorios de confianza: tratará los requisitos técnicos que deberán cumplir las referencias a documentos al ser intercambiadas, de forma que se evite trasladar documentación de forma innecesaria.

v) Norma Técnica de Política de firma electrónica y de certificados en el ámbito estatal: tratará las directrices y normas técnicas aplicables a la utilización de certificados y firma electrónica dentro de su ámbito de aplicación, organizadas alrededor de los conceptos de generación y validación de firma e incluirá los perfiles interoperables de los medios de identificación de las Administraciones Públicas previstos en Ley 40/2015, de 1 de octubre.

2. El Ministerio para la Transformación Digital y de la Función Pública, a propuesta de la Comisión Sectorial de Administración Electrónica prevista en la disposición adicional novena de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, aprobará las normas técnicas de interoperabilidad y las publicará mediante Resolución de la persona titular de la Secretaría de Estado de Función Pública.

3. Para la redacción y actualización de las normas técnicas de interoperabilidad indicadas en el apartado 1 y las futuras que pueda aprobar el Ministerio de Asuntos Económicos y Transformación Digital que sean necesarias para garantizar el adecuado nivel de interoperabilidad como consecuencia del nivel de desarrollo tecnológico, los compromisos internacionales o el marco normativo aplicable, se constituirán los correspondientes grupos de trabajo en los órganos colegiados con competencias en materia de Administración electrónica.

Para garantizar la debida interoperabilidad en materia de ciberseguridad y criptografía, en relación con la aplicación del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la administración electrónica, el órgano competente será el Centro Criptológico Nacional, adscrito al Centro Nacional de Inteligencia.

4. Se desarrollarán los siguientes instrumentos para la interoperabilidad:

a) Sistema de Información Administrativa: Inventario de procedimientos administrativos, servicios prestados y otras actuaciones administrativas que generen documentación pública, conteniendo información de los mismos clasificada por funciones y con indicación de su nivel de informatización, así como información acerca de las interfaces al objeto de favorecer la interacción o en su caso la integración de los procesos.

b) Centro de interoperabilidad semántica de la Administración: Almacenará, publicará y difundirá los modelos de datos de los servicios de interoperabilidad entre Administraciones Públicas y de estas con los ciudadanos, tanto comunes como sectoriales, así como los relativos a infraestructuras y servicios comunes, además de las especificaciones semánticas y codificaciones relacionadas. Su propósito es facilitar la comprensión semántica de los servicios de intercambio de datos de las Administraciones y maximizar la reutilización de activos semánticos en la construcción de éstos. Se conectará con otros instrumentos equivalentes de las Administraciones Públicas y del ámbito de la Unión Europea.

c) Centro de Transferencia de Tecnología: Directorio de aplicaciones para su libre reutilización que contendrá la relación de aplicaciones para su libre reutilización, incluyendo, al menos, los datos descriptivos relativos a nombre de la aplicación, breve descripción de sus funcionalidades, uso y características, licencia, principales estándares abiertos aplicados, y estado de desarrollo.

d) Directorio Común de Unidades Orgánicas y Oficinas de las Administraciones Públicas: Instrumento que permitirá la sincronización de los sistemas que traten la información de inventariado, codificación y evolución de unidades orgánicas y oficinas en diferentes modalidades de integración para garantizar la flexibilidad tanto en el consumo como en la provisión de información relacionada.

Disposición adicional segunda. *Formación.*

El personal de las Administraciones públicas recibirá la formación necesaria para garantizar el conocimiento del presente Esquema Nacional de Interoperabilidad, a cuyo fin los órganos responsables dispondrán lo necesario para que esta formación sea una realidad efectiva.

Disposición adicional tercera. *Centro Nacional de Referencia de Aplicación de las Tecnologías de la Información y la Comunicación (TIC) basadas en fuentes abiertas.*

(Suprimida)

Disposición adicional cuarta. *Instituto Nacional de Tecnologías de la Comunicación.*

(Suprimida)

Disposición adicional quinta. *Normativa técnica relativa a la reutilización de recursos de información.*

La normativa relativa a la reutilización de recursos de información deberá estar aprobada a más tardar el 1 de junio de 2012.

Disposición transitoria primera. *Adecuación de sistemas y servicios.*

Los sistemas existentes a la entrada en vigor del presente real decreto se adecuarán al Esquema Nacional de Interoperabilidad de forma que permitan el cumplimiento de lo establecido en la Disposición final tercera de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos. Los nuevos sistemas aplicarán lo establecido en el presente real decreto desde su concepción.

Si a los doce meses de la entrada en vigor del Esquema Nacional de Interoperabilidad hubiera circunstancias que impidan la plena aplicación de lo exigido en el mismo, se dispondrá de un plan de adecuación, que marque los plazos de ejecución los cuales, en ningún caso, serán superiores a 48 meses desde la entrada en vigor.

El plan indicado en el párrafo anterior será elaborado con la antelación suficiente y aprobado por los órganos superiores competentes.

Disposición transitoria segunda. *Uso de medios actualmente admitidos de identificación y autenticación.*

De acuerdo con lo previsto en el artículo 19 de la Ley 11/2007, de 22 de junio, y en la disposición transitoria primera del Real Decreto 1671/2009, de 6 de noviembre, se establece un plazo de adaptación de veinticuatro meses en el que se podrá seguir utilizando los medios actualmente admitidos de identificación y firma electrónica.

Disposición derogatoria única.

Quedan derogadas las disposiciones de igual o inferior rango que se opongan a lo dispuesto en el presente reglamento.

Disposición final primera. *Título habilitante.*

El presente real decreto se dicta en virtud de lo establecido en el artículo 149.1.18.ª de la Constitución, que atribuye al Estado la competencia sobre las bases del régimen jurídico de las Administraciones Públicas.

Disposición final segunda. *Desarrollo normativo.*

Se autoriza al titular del Ministerio de la Presidencia, para dictar las disposiciones necesarias para la aplicación y desarrollo de lo establecido en el presente real decreto, sin perjuicio de las competencias de las comunidades autónomas de desarrollo y ejecución de la legislación básica del Estado.

Disposición final tercera. *Entrada en vigor.*

El presente real decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

ANEXO

Glosario de términos

Aplicación: Programa o conjunto de programas cuyo objeto es la resolución de un problema mediante el uso de informática.

Aplicación de fuentes abiertas: Aquella que se distribuye con una licencia que permite la libertad de ejecutarla, de conocer el código fuente, de modificarla o mejorarla y de redistribuir copias a otros usuarios.

Cadena de interoperabilidad: Expresión de la interoperabilidad en el despliegue de los sistemas y los servicios como una sucesión de elementos enlazados e interconectados, de forma dinámica, a través de interfaces y con proyección a las dimensiones técnica, semántica y organizativa.

Ciclo de vida de un documento electrónico: Conjunto de las etapas o períodos por los que atraviesa la vida del documento, desde su identificación en un sistema de gestión de

documentos, hasta su selección para conservación permanente, de acuerdo con la legislación sobre Archivos de aplicación en cada caso, o para su destrucción reglamentaria.

Coste que no suponga una dificultad de acceso: Precio del estándar que, por estar vinculado al coste de distribución y no a su valor, no impide conseguir su posesión o uso.

Dato: Una representación de hechos, conceptos o instrucciones de un modo formalizado, y adecuado para comunicación, interpretación o procesamiento por medios automáticos o humanos.

Digitalización: El proceso tecnológico que permite convertir un documento en soporte papel o en otro soporte no electrónico en uno o varios ficheros electrónicos que contienen la imagen codificada, fiel e íntegra del documento.

Documento electrónico: Información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado.

Especificación técnica: Una especificación que figura en un documento en el que se definen las características requeridas de un producto, tales como los niveles de calidad, el uso específico, la seguridad o las dimensiones, incluidas las prescripciones aplicables al producto en lo referente a la denominación de venta, la terminología, los símbolos, los ensayos y métodos de ensayo, el envasado, el marcado y el etiquetado, así como los procedimientos de evaluación de la conformidad.

Especificación formalizada: Aquellas especificaciones que o bien son normas en el sentido de la Directiva 98/34 o bien proceden de consorcios de la industria u otros foros de normalización.

Esquema de metadatos: Instrumento que define la incorporación y gestión de los metadatos de contenido, contexto y estructura de los documentos electrónicos a lo largo de su ciclo de vida.

Estándar: Véase norma.

Estándar abierto: Aquél que reúne las siguientes condiciones:

a) Que sea público y su utilización sea disponible de manera gratuita o a un coste que no suponga una dificultad de acceso,

b) Que su uso y aplicación no esté condicionado al pago de un derecho de propiedad intelectual o industrial.

Ficheros de implementación de las políticas de firma: Son la representación en lenguaje formal (XML o ASN.1) de las condiciones establecidas en la política de firma, acorde a las normas técnicas establecidas por los organismos de estandarización.

Firma electrónica: Conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

Formato: Conjunto de reglas (algoritmo) que define la manera correcta de intercambiar o almacenar datos en memoria.

Herramientas genéricas: Instrumentos y programas de referencia, compartidos, de colaboración o componentes comunes y módulos similares reutilizables que satisfacen las necesidades comunes en los distintos ámbitos administrativos.

Imagen electrónica: Resultado de aplicar un proceso de digitalización a un documento.

Índice electrónico: Relación de documentos electrónicos de un expediente electrónico, firmada por la Administración, órgano o entidad actuante, según proceda y cuya finalidad es garantizar la integridad del expediente electrónico y permitir su recuperación siempre que sea preciso.

Infraestructura o servicio común: capacidad organizativa y técnica que satisface necesidades comunes de los usuarios en diversos ámbitos de la Administración, junto con su gobernanza operativa de apoyo, que pueden tener carácter horizontal o sectorial, con diversos modos de provisión, como servicio o como producto, o integración a modo de plataforma, que facilitan la interoperabilidad, la seguridad, las economías de escala, la racionalización y la simplificación de la actuación administrativa.

Interoperabilidad: Capacidad de los sistemas de información, y por ende de los procedimientos a los que éstos dan soporte, de compartir datos y posibilitar el intercambio de información y conocimiento entre ellos.

Interoperabilidad organizativa: Es aquella dimensión de la interoperabilidad relativa a la capacidad de las entidades y de los procesos a través de los cuales llevan a cabo sus

actividades para colaborar con el objeto de alcanzar logros mutuamente acordados relativos a los servicios que prestan.

Interoperabilidad semántica: Es aquella dimensión de la interoperabilidad relativa a que la información intercambiada pueda ser interpretable de forma automática y reutilizable por aplicaciones que no intervinieron en su creación.

Interoperabilidad técnica: Es aquella dimensión de la interoperabilidad relativa a la relación entre sistemas y servicios de tecnologías de la información, incluyendo aspectos tales como las interfaces, la interconexión, la integración de datos y servicios, la presentación de la información, la accesibilidad y la seguridad, u otros de naturaleza análoga.

Interoperabilidad en el tiempo: Es aquella dimensión de la interoperabilidad relativa a la interacción entre elementos que corresponden a diversas oleadas tecnológicas; se manifiesta especialmente en la conservación de la información en soporte electrónico.

Licencia Pública de la Unión Europea («European Union Public Licence-EUPL»): Licencia adoptada oficialmente por la Comisión Europea en las 22 lenguas oficiales comunitarias para reforzar la interoperabilidad de carácter legal mediante un marco colectivo para la puesta en común de las aplicaciones del sector público.

Lista de servicios de confianza (TSL): Lista de acceso público que recoge información precisa y actualizada de aquellos servicios de certificación y firma electrónica que se consideran aptos para su empleo en un marco de interoperabilidad de las Administraciones públicas españolas y europeas.

Marca de tiempo: La asignación por medios electrónicos de la fecha y, en su caso, la hora a un documento electrónico.

Medio electrónico: Mecanismo, instalación, equipo o sistema que permite producir, almacenar o transmitir documentos, datos e informaciones; incluyendo cualesquiera redes de comunicación abiertas o restringidas como Internet, telefonía fija y móvil u otras.

Metadato: Dato que define y describe otros datos. Existen diferentes tipos de metadatos según su aplicación.

Metadato de gestión de documentos: Información estructurada o semiestructurada que hace posible la creación, gestión y uso de documentos a lo largo del tiempo en el contexto de su creación. Los metadatos de gestión de documentos sirven para identificar, autenticar y contextualizar documentos, y del mismo modo a las personas, los procesos y los sistemas que los crean, gestionan, mantienen y utilizan.

Modelo de datos: Conjunto de definiciones (modelo conceptual), interrelaciones (modelo lógico) y reglas y convenciones (modelo físico) que permiten describir los datos para su intercambio.

Nivel de resolución: Resolución espacial de la imagen obtenida como resultado de un proceso de digitalización.

Nodo de interoperabilidad: Organismo que presta servicios de interconexión técnica, organizativa y jurídica entre sistemas de información para un conjunto de Administraciones Públicas bajo las condiciones que éstas fijen.

Norma: Especificación técnica aprobada por un organismo de normalización reconocido para una aplicación repetida o continuada cuyo cumplimiento no sea obligatorio y que esté incluida en una de las categorías siguientes:

a) norma internacional: norma adoptada por una organización internacional de normalización y puesta a disposición del público,

b) norma europea: norma adoptada por un organismo europeo de normalización y puesta a disposición del público,

c) norma nacional: norma adoptada por un organismo nacional de normalización y puesta a disposición del público.

Política de firma electrónica: Conjunto de normas de seguridad, de organización, técnicas y legales para determinar cómo se generan, verifican y gestionan firmas electrónicas, incluyendo las características exigibles a los certificados de firma.

Política de gestión de documentos electrónicos: Orientaciones o directrices que define una organización para la creación y gestión de documentos auténticos, fiables y disponibles a lo largo del tiempo, de acuerdo con las funciones y actividades que le son propias. La

política se aprueba al más alto nivel dentro de la organización, y asigna responsabilidades en cuanto a la coordinación, aplicación, supervisión y gestión del programa de tratamiento de los documentos a través de su ciclo de vida.

Procedimiento administrativo: Proceso formal regulado jurídicamente para la toma de decisiones por parte de las Administraciones públicas para garantizar la legalidad, eficacia, eficiencia, calidad, derechos e intereses presentes, que termina con una resolución en la que se recoge un acto administrativo; este proceso formal jurídicamente regulado se implementa en la práctica mediante un proceso operativo que coincide en mayor o menor medida con el formal.

Proceso operativo: Conjunto organizado de actividades que se llevan a cabo para producir un producto o servicio; tiene un principio y fin delimitado, implica recursos y da lugar a un resultado.

Repositorio electrónico: Archivo centralizado donde se almacenan y administran datos y documentos electrónicos, y sus metadatos.

Sello de tiempo: La asignación por medios electrónicos de una fecha y hora a un documento electrónico con la intervención de un prestador de servicios de certificación que asegure la exactitud e integridad de la marca de tiempo del documento.

Sellado de tiempo: Acreditación a cargo de un tercero de confianza de la fecha y hora de realización de cualquier operación o transacción por medios electrónicos.

Servicio de interoperabilidad: Cualquier mecanismo que permita a las Administraciones públicas compartir datos e intercambiar información mediante el uso de las tecnologías de la información.

Soporte: Objeto sobre el cual o en el cual es posible grabar y recuperar datos.

Trámite: Cada uno de los estados y diligencias que hay que recorrer en un negocio hasta su conclusión.

Uso generalizado por los ciudadanos: Usado por casi todas las personas físicas, personas jurídicas y entes sin personalidad que se relacionen o sean susceptibles de relacionarse con las Administraciones públicas españolas.

§ 11

Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información

Jefatura del Estado
«BOE» núm. 218, de 8 de septiembre de 2018
Última modificación: 30 de marzo de 2022
Referencia: BOE-A-2018-12257

I

La evolución de las tecnologías de la información y de la comunicación, especialmente con el desarrollo de Internet, ha hecho que las redes y sistemas de información desempeñen actualmente un papel crucial en nuestra sociedad, siendo su fiabilidad y seguridad aspectos esenciales para el desarrollo normal de las actividades económicas y sociales.

Por ello, los incidentes que, al afectar a las redes y sistemas de información, alteran dichas actividades, representan una grave amenaza, pues tanto si son fortuitos como si provienen de acciones deliberadas pueden generar pérdidas financieras, menoscabar la confianza de la población y, en definitiva, causar graves daños a la economía y a la sociedad, con la posibilidad de afectar a la propia seguridad nacional en la peor de las hipótesis.

El carácter transversal e interconectado de las tecnologías de la información y de la comunicación, que también caracteriza a sus amenazas y riesgos, limita la eficacia de las medidas que se emplean para contrarrestarlos cuando se toman de modo aislado. Este carácter transversal también hace que se corra el riesgo de perder efectividad si los requisitos en materia de seguridad de la información se definen de forma independiente para cada uno de los ámbitos sectoriales afectados.

Por tanto, es oportuno establecer mecanismos que, con una perspectiva integral, permitan mejorar la protección frente a las amenazas que afectan a las redes y sistemas de información, facilitando la coordinación de las actuaciones realizadas en esta materia tanto a nivel nacional como con los países de nuestro entorno, en particular, dentro de la Unión Europea.

II

Con este propósito se dicta este real decreto-ley, que transpone al ordenamiento jurídico español la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. El real decreto-ley se apoya igualmente en las normas, en los instrumentos de respuesta a incidentes y en los órganos de coordinación estatal existentes en esta materia, lo que, junto a las razones señaladas en el apartado I, justifica que su contenido trascienda el de la propia Directiva.

El real decreto-ley se aplicará a las entidades que presten servicios esenciales para la comunidad y dependan de las redes y sistemas de información para el desarrollo de su actividad. Su ámbito de aplicación se extiende a sectores que no están expresamente incluidos en la Directiva, para darle a este real decreto-ley un enfoque global, aunque se preserva su legislación específica. Adicionalmente, en el caso de las actividades de explotación de las redes y de prestación de servicios de comunicaciones electrónicas y los recursos asociados, así como de los servicios electrónicos de confianza, expresamente excluidos de dicha Directiva, el real decreto-ley se aplicará únicamente en lo que respecta a los operadores críticos.

El real decreto-ley se aplicará, así mismo, a los proveedores de determinados servicios digitales. La Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, los somete a un régimen de armonización máxima, equivalente a un reglamento, pues se considera que su regulación a escala nacional no sería efectiva por tener un carácter intrínsecamente transnacional. La función de las autoridades nacionales se limita, por tanto, a supervisar su aplicación por los proveedores establecidos en su país, y coordinarse con las autoridades correspondientes de otros países de la Unión Europea.

Siguiendo la citada Directiva, el real decreto-ley identifica los sectores en los que es necesario garantizar la protección de las redes y sistemas de información, y establece procedimientos para identificar los servicios esenciales ofrecidos en dichos sectores, así como los principales operadores que prestan dichos servicios, que son, en definitiva, los destinatarios de este real decreto-ley.

Los operadores de servicios esenciales y los proveedores de servicios digitales deberán adoptar medidas adecuadas para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información que utilicen, aunque su gestión esté externalizada. Las obligaciones de seguridad que asuman deberán ser proporcionadas al nivel de riesgo que afronten y estar basadas en una evaluación previa de los mismos. Las normas de desarrollo de este real decreto-ley podrán concretar las obligaciones de seguridad exigibles a los operadores de servicios esenciales, incluyendo en su caso las inspecciones a realizar o la participación en actividades y ejercicios de gestión de crisis.

El real decreto-ley requiere así mismo que los operadores de servicios esenciales y los proveedores de servicios digitales notifiquen los incidentes que sufran en las redes y servicios de información que emplean para la prestación de los servicios esenciales y digitales, y tengan efectos perturbadores significativos en los mismos, al tiempo que prevé la notificación de los sucesos o incidencias que puedan afectar a los servicios esenciales, pero que aún no hayan tenido un efecto adverso real sobre aquellos, y perfila los procedimientos de notificación.

La notificación de incidentes forma parte de la cultura de gestión de riesgos que la Directiva y el real decreto-ley fomentan. Por ello, el real decreto-ley protege a la entidad notificante y al personal que informe sobre incidentes ocurridos; se reserva la información confidencial de su divulgación al público o a otras autoridades distintas de la notificada y se permite la notificación de incidentes cuando no sea obligada su comunicación.

El real decreto-ley recalca la necesidad de tener en cuenta los estándares europeos e internacionales, así como las recomendaciones que emanen del grupo de cooperación y de la red de CSIRT (Computer Security Incident Response Team) establecidos en el ámbito comunitario por la Directiva, con vistas a aplicar las mejores prácticas aprendidas en estos foros y contribuir al impulso del mercado interior y a la participación de nuestras empresas en él.

Con el fin de aumentar su eficacia y, al tiempo, reducir las cargas administrativas y económicas que estas obligaciones suponen para las entidades afectadas, este real decreto-ley trata de garantizar su coherencia con las que se derivan de la aplicación de otras normativas en materia de seguridad de la información, tanto de carácter horizontal como sectorial, y la coordinación en su aplicación con las autoridades responsables en cada caso.

Respecto a las normas horizontales, destacan los vínculos establecidos con las Leyes 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, y 36/2015, de 28 de septiembre, de Seguridad Nacional, y con el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad

en el ámbito de la Administración Electrónica, como normativa especial en materia de seguridad de los sistemas de información del sector público.

Así, se aproxima el ámbito de aplicación de este real decreto-ley al de la Ley 8/2011, de 28 de abril, añadiendo a los sectores previstos por la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, los sectores estratégicos adicionales contemplados en esa ley; se apoya en ella para definir el concepto de «servicio esencial», y se atribuye a sus órganos colegiados la determinación de los servicios esenciales y de los operadores de servicios esenciales sujetos al presente real decreto-ley. Teniendo en cuenta la Ley 36/2015, de 28 de septiembre, se atribuye al Consejo de Seguridad Nacional la función de actuar como punto de contacto con otros países de la Unión Europea y un papel coordinador de la política de ciberseguridad a través de la Estrategia de Ciberseguridad Nacional.

III

La Estrategia de Ciberseguridad Nacional con la que España cuenta desde el año 2013, sienta las prioridades, objetivos y medidas adecuadas para alcanzar y mantener un elevado nivel de seguridad de las redes y sistemas de información. Dicha Estrategia seguirá desarrollando el marco institucional de la ciberseguridad que este real decreto-ley esboza, compuesto por las autoridades públicas competentes y los CSIRT de referencia, por una parte, y la cooperación público-privada, por otra.

Las autoridades competentes ejercerán las funciones de vigilancia derivadas de este real decreto-ley y aplicarán el régimen sancionador cuando proceda. Así mismo, promoverán el desarrollo de las obligaciones que el real decreto-ley impone, en consulta con el sector y con las autoridades que ejerzan competencias por razón de la materia cuando se refieran a sectores específicos, para evitar la existencia de obligaciones duplicadas, innecesarias o excesivamente onerosas.

Los CSIRT son los equipos de respuesta a incidentes que analizan riesgos y supervisan incidentes a escala nacional, difunden alertas sobre ellos y aportan soluciones para mitigar sus efectos. El término CSIRT es el usado comúnmente en Europa en lugar del término protegido CERT (Computer Emergency Response Team), registrado en EE.UU.

El real decreto-ley delimita el ámbito funcional de actuación de los CSIRT de referencia previstos en ella. Dichos CSIRT son la puerta de entrada de las notificaciones de incidentes, lo que permitirá organizar rápidamente la respuesta a ellos, pero el destinatario de las notificaciones es la autoridad competente respectiva, que tendrá en cuenta esta información para la supervisión de los operadores. En todo caso, el operador es responsable de resolver los incidentes y reponer las redes y sistemas de información afectados a su funcionamiento ordinario.

Se prevé la utilización de una plataforma común para la notificación de incidentes, de tal manera que los operadores no deban efectuar varias notificaciones en función de la autoridad a la que deban dirigirse. Esta plataforma podrá ser empleada también para la notificación de vulneraciones de la seguridad de datos personales según el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

IV

Este real decreto-ley consta de siete títulos que contienen, en primer lugar, las definiciones de los términos que se usan a lo largo del texto, la salvaguarda de funciones estatales esenciales, como la seguridad nacional y otras disposiciones generales. A continuación, en el título II se determina la forma y criterios de identificación de los servicios esenciales y de los operadores que los presten a los que se aplicará el real decreto-ley. El orden en que se procederá a su identificación por primera vez se establece en la disposición adicional primera del real decreto-ley. El título III recoge el marco estratégico e institucional de la seguridad de las redes y sistemas de información que se ha descrito anteriormente. Se dedica un precepto específico a la cooperación entre autoridades públicas, como pilar de un ejercicio adecuado de las diferentes competencias concurrentes sobre la materia.

El título IV se ocupa de las obligaciones de seguridad de los operadores, y en él se prevé la aplicación preferente de normas sectoriales que impongan obligaciones equivalentes a las previstas en este real decreto-ley, sin perjuicio de la coordinación ejercida por el Consejo de Seguridad Nacional y del deber de cooperación con las autoridades competentes en virtud de este real decreto-ley.

En el título V, el más extenso, se regula la notificación de incidentes y se presta atención a los incidentes con impacto transfronterizo y a la información y coordinación con otros Estados de la Unión Europea para su gestión. En el título VI, se disponen las potestades de inspección y control de las autoridades competentes y la cooperación con las autoridades nacionales de otros Estados miembros, y en el título VII se tipifican las infracciones y sanciones de este real decreto-ley. En este aspecto, el real decreto-ley se decanta por impulsar la subsanación de la infracción antes que su castigo, el cual, si es necesario dispensarlo, será efectivo, proporcionado y disuasorio, en línea con lo ordenado por la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016.

El real decreto-ley se cierra con una parte final que incluye las disposiciones adicionales y finales necesarias para completar la regulación.

Esta disposición ha sido sometida al procedimiento de información de normas reglamentarias técnicas y de reglamentos relativos a los servicios de la sociedad de la información, previsto en la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo, de 9 de septiembre de 2015, por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información, así como el Real Decreto 1337/1999, de 31 de julio, por el que se regula la remisión de información en materia de normas y reglamentaciones técnicas y reglamentos relativos a los servicios de la sociedad de la información. Así mismo, se adecúa a los principios de buena regulación establecidos en el artículo 129 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, conforme a los cuales deben actuar las Administraciones Públicas en el ejercicio de la iniciativa legislativa, como son los principios de necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia y eficiencia.

Este real decreto-ley se dicta en virtud de las competencias exclusivas atribuidas al Estado en materia de régimen general de telecomunicaciones y seguridad pública por el artículo 149.1.21.ª y 29.ª de la Constitución.

El real decreto-ley constituye un instrumento constitucionalmente lícito, siempre que el fin que justifica la legislación de urgencia, sea, tal como reiteradamente ha exigido nuestro Tribunal Constitucional (Sentencias 6/1983, de 4 de febrero, F. 5; 11/2002, de 17 de enero, F. 4, 137/2003, de 3 de julio, F. 3 y 189/2005, de 7 julio, F.3), subvenir a un situación concreta, dentro de los objetivos gubernamentales, que por razones difíciles de prever requiere una acción normativa inmediata en un plazo más breve que el requerido por la vía normal o por el procedimiento de urgencia para la tramitación parlamentaria de las Leyes.

Por otro lado, la utilización del instrumento jurídico del real decreto-ley, en el presente caso, además queda justificada por la doctrina del Tribunal Constitucional, que, en su Sentencia 1/2012, de 13 de enero, ha avalado la concurrencia del presupuesto habilitante de la extraordinaria y urgente necesidad del artículo 86.1 de la Constitución, cuando concurra el retraso en la transposición de directivas.

En efecto, el plazo de transposición de la mencionada Directiva (UE) 2016/1148, del Parlamento Europeo y del Consejo, de 6 de julio de 2016, se encuentra ya vencido a 9 de mayo de 2018. La finalización del plazo de transposición de esta Directiva ha motivado la iniciación por parte de la Comisión Europea de un procedimiento formal de infracción n.º 2018/168.

En consecuencia, se entiende que en el conjunto y en cada una de las medidas que se adoptan mediante el real decreto-ley proyectado, concurren, por su naturaleza y finalidad, las circunstancias de extraordinaria y urgente necesidad que exige el artículo 86 de la Constitución como presupuestos habilitantes para la aprobación de un real decreto-ley.

En su virtud, haciendo uso de la autorización contenida en el artículo 86 de la Constitución Española, a propuesta de la Vicepresidenta del Gobierno y Ministra de la Presidencia, Relaciones con las Cortes e Igualdad, del Ministro del Interior y de la Ministra

de Economía y Empresa y previa deliberación del Consejo de Ministros, en su reunión del día 7 de septiembre de 2018,

DISPONGO:

TÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

1. El presente real decreto-ley tiene por objeto regular la seguridad de las redes y sistemas de información utilizados para la provisión de los servicios esenciales y de los servicios digitales, y establecer un sistema de notificación de incidentes.

2. Así mismo, establece un marco institucional para la aplicación de este real decreto-ley y la coordinación entre autoridades competentes y con los órganos de cooperación relevantes en el ámbito comunitario.

Artículo 2. *Ámbito de aplicación.*

1. Este real decreto-ley se aplicará a la prestación de:

a) Los servicios esenciales dependientes de las redes y sistemas de información comprendidos en los sectores estratégicos definidos en el anexo de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

b) Los servicios digitales, considerados conforme se determina en el artículo 3 e), que sean mercados en línea, motores de búsqueda en línea y servicios de computación en nube.

2. Estarán sometidos a este real decreto-ley:

a) Los operadores de servicios esenciales establecidos en España. Se entenderá que un operador de servicios esenciales está establecido en España cuando su residencia o domicilio social se encuentren en territorio español, siempre que éstos coincidan con el lugar en que esté efectivamente centralizada la gestión administrativa y la dirección de sus negocios o actividades.

Así mismo, este real decreto-ley será de aplicación a los servicios esenciales que los operadores residentes o domiciliados en otro Estado ofrezcan a través de un establecimiento permanente situado en España.

b) Los proveedores de servicios digitales que tengan su sede social en España y que constituya su establecimiento principal en la Unión Europea, así como los que, no estando establecidos en la Unión Europea, designen en España a su representante en la Unión para el cumplimiento de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

3. Este real decreto-ley no se aplicará a:

a) Los operadores de redes y servicios de comunicaciones electrónicas y los prestadores de servicios electrónicos de confianza que no sean designados como operadores críticos en virtud de la Ley 8/2011, de 28 de abril.

b) Los proveedores de servicios digitales cuando se trate de microempresas o pequeñas empresas, de acuerdo con las definiciones recogidas en la Recomendación 2003/361/CE de la Comisión, de 6 de mayo de 2003, sobre la definición de microempresas, pequeñas y medianas empresas.

Artículo 3. *Definiciones.*

A los efectos de este real decreto-ley, se entenderá por:

a) Redes y sistemas de información, cualquiera de los elementos siguientes:

1.º Las redes de comunicaciones electrónicas, tal y como vienen definidas en el número 31 del anexo II de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones;

2.º Todo dispositivo o grupo de dispositivos interconectados o relacionados entre sí, en el que uno o varios de ellos realicen, mediante un programa, el tratamiento automático de datos digitales;

3.º Los datos digitales almacenados, tratados, recuperados o transmitidos mediante los elementos contemplados en los números 1.º y 2.º anteriores, incluidos los necesarios para el funcionamiento, utilización, protección y mantenimiento de dichos elementos.

b) Seguridad de las redes y sistemas de información: la capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos.

c) Servicio esencial: servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas, que dependa para su provisión de redes y sistemas de información.

d) Operador de servicios esenciales: entidad pública o privada que se identifique considerando los factores establecidos en el artículo 6 de este real decreto-ley, que preste dichos servicios en alguno de los sectores estratégicos definidos en el anexo de la Ley 8/2011, de 28 de abril.

e) Servicio digital: servicio de la sociedad de la información entendido en el sentido recogido en la letra a) del anexo de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

f) Proveedor de servicios digitales: persona jurídica que presta un servicio digital.

g) Riesgo: toda circunstancia o hecho razonablemente identificable que tenga un posible efecto adverso en la seguridad de las redes y sistemas de información. Se puede cuantificar como la probabilidad de materialización de una amenaza que produzca un impacto en términos de operatividad, de integridad física de personas o material o de imagen.

h) Incidente: suceso inesperado o no deseado con consecuencias en detrimento de la seguridad de las redes y sistemas de información.

i) Gestión de incidentes: procedimientos seguidos para detectar, analizar y limitar un incidente y responder ante éste.

j) Representante: persona física o jurídica establecida en la Unión Europea que ha sido designada expresamente para actuar por cuenta de un proveedor de servicios digitales no establecido en la Unión Europea, a la que, en sustitución del proveedor de servicios digitales, pueda dirigirse una autoridad competente nacional o un CSIRT, en relación con las obligaciones que, en virtud de este real decreto-ley, tiene el proveedor de servicios digitales.

k) Norma técnica: una norma en el sentido del artículo 2.1 del Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, sobre la normalización europea.

l) Especificación: una especificación técnica en el sentido del artículo 2.4 del Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo, de 25 de octubre de 2012.

m) Punto de intercambio de Internet («IXP», por sus siglas en inglés de «Internet eXchange Point»): una instalación de red que permite interconectar más de dos sistemas autónomos independientes, principalmente para facilitar el intercambio de tráfico de Internet. Un IXP permite interconectar sistemas autónomos sin requerir que el tráfico de Internet que pasa entre cualquier par de sistemas autónomos participantes pase por un tercer sistema autónomo, y sin modificar ni interferir de otra forma en dicho tráfico.

n) Sistema de nombres de dominio («DNS», por sus siglas en inglés de «Domain Name System»): sistema distribuido jerárquicamente que responde a consultas proporcionando información asociada a nombres de dominio, en particular, la relativa a los identificadores utilizados para localizar y direccionar equipos en Internet.

o) Proveedor de servicios de DNS: entidad que presta servicios de DNS en Internet.

p) Registro de nombres de dominio de primer nivel: entidad que administra y dirige el registro de nombres de dominio de Internet en un dominio específico de primer nivel.

q) Mercado en línea: servicio digital que permite a los consumidores y a los empresarios, tal y como se definen respectivamente en los artículos 3 y 4 del texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, aprobado mediante el Real Decreto Legislativo 1/2007, de 16 de noviembre, celebrar entre sí contratos de compraventa o de prestación de servicios en línea con empresarios, ya sea en un sitio web específico del servicio de mercado en línea, o en un sitio web de un empresario que utilice servicios informáticos proporcionados al efecto por el proveedor del servicio de mercado en línea.

r) Motor de búsqueda en línea: servicio digital que permite a los usuarios hacer búsquedas de, en principio, todos los sitios web o de sitios web en una lengua en concreto, mediante una consulta sobre un tema en forma de palabra clave, frase u otro tipo de entrada, y que, en respuesta, muestra enlaces en los que puede encontrarse información relacionada con el contenido solicitado.

s) Servicio de computación en nube: servicio digital que hace posible el acceso a un conjunto modulable y elástico de recursos de computación que se pueden compartir.

Artículo 4. *Directrices y orientaciones comunitarias.*

En la aplicación de este real decreto-ley y en la elaboración de los reglamentos y guías previstos en él se tendrán en cuenta los actos de ejecución de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, así como todas las recomendaciones y directrices emanadas del grupo de cooperación establecido por el artículo 11 de la citada Directiva, y la información sobre buenas prácticas recopiladas por dicho grupo y la red de CSIRT, regulado en el artículo 12 de aquélla.

Artículo 5. *Salvaguarda de funciones estatales esenciales.*

Lo dispuesto en este real decreto-ley se entenderá sin perjuicio de las acciones emprendidas para salvaguardar la seguridad nacional y las funciones estatales esenciales, incluyéndose las dirigidas a proteger la información clasificada o cuya revelación fuere contraria a los intereses esenciales del Estado, o las que tengan como propósito el mantenimiento del orden público, la detección, investigación y persecución de los delitos, y el enjuiciamiento de sus autores.

TÍTULO II

Servicios esenciales y servicios digitales

Artículo 6. *Identificación de servicios esenciales y de operadores de servicios esenciales.*

1. La identificación de los servicios esenciales y de los operadores que los presten se efectuará por los órganos y procedimientos previstos por la Ley 8/2011, de 28 de abril, y su normativa de desarrollo.

La relación de los servicios esenciales y de los operadores de dichos servicios se actualizará, para cada sector, con una frecuencia bienal, en conjunción con la revisión de los planes estratégicos sectoriales previstos en la Ley 8/2011, de 28 de abril.

Se identificará a un operador como operador de servicios esenciales si un incidente sufrido por el operador puede llegar a tener efectos perturbadores significativos en la prestación del servicio, para lo que se tendrán en cuenta, al menos, los siguientes factores:

a) En relación con la importancia del servicio prestado:

1.º La disponibilidad de alternativas para mantener un nivel suficiente de prestación del servicio esencial;

2.º La valoración del impacto de un incidente en la provisión del servicio, evaluando la extensión o zonas geográficas que podrían verse afectadas por el incidente; la dependencia de otros sectores estratégicos respecto del servicio esencial ofrecido por la entidad y la repercusión, en términos de grado y duración, del incidente en las actividades económicas y sociales o en la seguridad pública.

b) En relación con los clientes de la entidad evaluada:

1.º El número de usuarios que confían en los servicios prestados por ella;
2.º Su cuota de mercado.

Reglamentariamente podrán añadirse factores específicos del sector para determinar si un incidente podría tener efectos perturbadores significativos.

2. En el caso de tratarse de un operador crítico designado en cumplimiento de la Ley 8/2011, de 28 de abril, bastará con que se constate su dependencia de las redes y sistemas de información para la provisión del servicio esencial de que se trate.
3. En la identificación de los servicios esenciales y de los operadores de servicios esenciales se tendrán en consideración, en la mayor medida posible, las recomendaciones pertinentes que adopte el grupo de cooperación.
4. Cuando un operador de servicios esenciales ofrezca servicios en otros Estados miembros de la Unión Europea, se informará a los puntos de contacto único de dichos Estados sobre la intención de identificarlo como operador de servicios esenciales.

Artículo 7. *Comunicación de actividad por los proveedores de servicios digitales.*

Los proveedores de servicios digitales señalados en el artículo 2 deberán comunicar su actividad a la autoridad competente en el plazo de tres meses desde que la inicien, a los meros efectos de su conocimiento.

TÍTULO III

Marco estratégico e institucional

Artículo 8. *Marco estratégico de seguridad de las redes y sistemas de información.*

La Estrategia de Ciberseguridad Nacional, al amparo y alineada con la Estrategia de Seguridad Nacional, enmarca los objetivos y las medidas para alcanzar y mantener un elevado nivel de seguridad de las redes y sistemas de información.
La Estrategia de Ciberseguridad Nacional abordará, entre otras cuestiones, las establecidas en el artículo 7 de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016.
A tal efecto, el Consejo de Seguridad Nacional impulsará la revisión de la Estrategia de Ciberseguridad Nacional, de conformidad con lo dispuesto en el artículo 21.1 e) de la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.

Artículo 9. *Autoridades competentes.*

1. Son autoridades competentes en materia de seguridad de las redes y sistemas de información las siguientes:

a) Para los operadores de servicios esenciales:

1.º En el caso de que éstos sean, además, designados como operadores críticos conforme a la Ley 8/2011, de 28 de abril, y su normativa de desarrollo, con independencia del sector estratégico en que se realice tal designación: la Secretaría de Estado de Seguridad, del Ministerio del Interior, a través del Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC).
2.º En el caso de que no sean operadores críticos: la autoridad sectorial correspondiente por razón de la materia, según se determine reglamentariamente.

b) Para los proveedores de servicios digitales: la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital.
c) Para los operadores de servicios esenciales y proveedores de servicios digitales que no siendo operadores críticos se encuentren comprendidos en el ámbito de aplicación de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público: el Ministerio de Defensa, a través del Centro Criptológico Nacional.

2. El Consejo de Seguridad Nacional, a través de su comité especializado en materia de ciberseguridad, establecerá los mecanismos necesarios para la coordinación de las actuaciones de las autoridades competentes.

Artículo 10. *Funciones de las autoridades competentes.*

Las autoridades competentes ejercerán las siguientes funciones:

a) Supervisar el cumplimiento por parte de los operadores de servicios esenciales y de los proveedores de servicios digitales de las obligaciones que se determinen, conforme a lo establecido en el título VI.

b) Establecer canales de comunicación oportunos con los operadores de servicios esenciales y con los proveedores de servicios digitales que, en su caso, serán desarrollados reglamentariamente.

c) Coordinarse con los CSIRT de referencia a través de los protocolos de actuación que, en su caso, se desarrollarán reglamentariamente.

d) Recibir las notificaciones sobre incidentes que sean presentadas en el marco de este real decreto-ley, a través de los CSIRT de referencia, conforme a lo establecido en el título V.

e) Informar al punto de contacto único sobre las notificaciones de incidentes presentadas en el marco de este real decreto-ley, conforme a lo establecido en el artículo 27.

f) Informar, en su caso, al público sobre determinados incidentes, cuando la difusión de dicha información sea necesaria para evitar un incidente o gestionar uno que ya se haya producido, conforme a lo establecido en el artículo 26.

g) Cooperar, en el ámbito de aplicación de este real decreto-ley, con las autoridades competentes en materia de protección de datos de carácter personal, seguridad pública, seguridad ciudadana y seguridad nacional, así como con las autoridades sectoriales correspondientes, conforme a lo establecido en los artículos 14 y 29.

h) Establecer obligaciones específicas para garantizar la seguridad de las redes y sistemas de información y sobre notificación de incidentes, y dictar instrucciones técnicas y guías orientativas para detallar el contenido de dichas obligaciones, conforme a lo establecido en los artículos 16 y 19.

i) Ejercer la potestad sancionadora en los casos previstos en el presente real decreto-ley, conforme a lo establecido en el título VII.

j) Promover el uso de normas y especificaciones técnicas, de acuerdo con lo establecido en el artículo 17.

k) Cooperar con las autoridades competentes de otros Estados miembros de la Unión Europea en la identificación de operadores de servicios esenciales entre entidades que ofrezcan dichos servicios en varios Estados miembros.

l) Informar al punto de contacto único sobre incidentes que puedan afectar a otros Estados miembros, en los términos previstos en el artículo 25.

Artículo 11. *Equipos de respuesta a incidentes de seguridad informática de referencia.*

1. Son equipos de respuesta a incidentes de seguridad informática (CSIRT) de referencia en materia de seguridad de las redes y sistemas de información, los siguientes:

a) En lo concerniente a las relaciones con los operadores de servicios esenciales:

1.º El CCN-CERT, del Centro Criptológico Nacional, al que corresponde la comunidad de referencia constituida por las entidades del ámbito subjetivo de aplicación de la Ley 40/2015, de 1 de octubre.

2.º El INCIBE-CERT, del Instituto Nacional de Ciberseguridad de España, al que corresponde la comunidad de referencia constituida por aquellas entidades no incluidas en el ámbito subjetivo de aplicación de la Ley 40/2015, de 1 de octubre.

El INCIBE-CERT será operado conjuntamente por el INCIBE y el CNPIC en todo lo que se refiera a la gestión de incidentes que afecten a los operadores críticos.

3.º El ESPDEF-CERT, del Ministerio de Defensa, que cooperará con el CCN-CERT y el INCIBE-CERT en aquellas situaciones que éstos requieran en apoyo de los operadores de servicios esenciales y, necesariamente, en aquellos operadores que tengan incidencia en la Defensa Nacional y que reglamentariamente se determinen.

b) En lo concerniente a las relaciones con los proveedores de servicios digitales que no estuvieren comprendidos en la comunidad de referencia del CCN-CERT: el INCIBE-CERT.

El INCIBE-CERT será, así mismo, equipo de respuesta a incidentes de referencia para los ciudadanos, entidades de derecho privado y otras entidades no incluidas anteriormente en este apartado 1.

2. Los CSIRT de referencia se coordinarán entre sí y con el resto de CSIRT nacionales e internacionales en la respuesta a los incidentes y gestión de riesgos de seguridad que les correspondan. En los supuestos de especial gravedad que reglamentariamente se determinen y que requieran un nivel de coordinación superior al necesario en situaciones ordinarias, el CCN-CERT ejercerá la coordinación nacional de la respuesta técnica de los CSIRT.

Cuando las actividades que desarrollen puedan afectar de alguna manera a un operador crítico, los CSIRT de referencia se coordinarán con el Ministerio del Interior, a través de la Oficina de Coordinación Cibernética del Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC), de la forma que reglamentariamente se determine.

3. El Centro Criptológico Nacional (CCN) ejercerá la coordinación nacional de la respuesta técnica de los equipos de respuesta a incidentes de seguridad informática (CSIRT) en materia de seguridad de las redes y sistemas de información del sector público comprendido en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Los CSIRT de las Administraciones Públicas consultarán, cuando proceda, con los órganos con competencias en materia de seguridad nacional, seguridad pública, seguridad ciudadana y protección de datos de carácter personal y colaborarán con ellos en el ejercicio de sus respectivas funciones.

El CCN ejercerá la función de enlace para garantizar la cooperación transfronteriza de los CSIRT de las Administraciones Públicas con los CSIRT internacionales, en la respuesta a los incidentes y gestión de riesgos de seguridad que les correspondan.

Artículo 12. *Requisitos y funciones de los CSIRT de referencia.*

1. Los CSIRT deberán reunir las siguientes condiciones:

a) Garantizarán un elevado nivel de disponibilidad de sus servicios de comunicaciones evitando los fallos ocasionales y contarán con varios medios para que se les pueda contactar y puedan contactar a otros en todo momento. Además, los canales de comunicación estarán claramente especificados y serán bien conocidos de los grupos de usuarios y los socios colaboradores.

b) Sus instalaciones y las de los sistemas de información de apoyo estarán situados en lugares seguros.

c) Garantizarán la continuidad de las actividades. Para ello:

1.º Estarán dotados de un sistema adecuado para gestionar y canalizar las solicitudes con el fin de facilitar los traspasos.

2.º Contarán con personal suficiente para garantizar su disponibilidad en todo momento.

3.º Tendrán acceso a infraestructuras de comunicación cuya continuidad esté asegurada. A tal fin, dispondrán de sistemas redundantes y espacios de trabajo de reserva.

d) Deberán tener la capacidad de participar, cuando lo deseen, en redes de cooperación internacional.

2. Los CSIRT desempeñarán como mínimo, las siguientes funciones:

a) Supervisar incidentes a escala nacional.

b) Difundir alertas tempranas, alertas, avisos e información sobre riesgos e incidentes entre los interesados.

c) Responder a incidentes.

d) Efectuar un análisis dinámico de riesgos e incidentes y de conocimiento de la situación.

e) Participar en la red de CSIRT.

3. Los CSIRT establecerán relaciones de cooperación con el sector privado. A fin de facilitar la cooperación, los CSIRT fomentarán la adopción y utilización de prácticas comunes o normalizadas de:

a) Procedimientos de gestión de incidentes y riesgos.
b) Sistemas de clasificación de incidentes, riesgos e información.

Artículo 13. *Punto de contacto único.*

El Consejo de Seguridad Nacional ejercerá, a través del Departamento de Seguridad Nacional, una función de enlace para garantizar la cooperación transfronteriza de las autoridades competentes designadas conforme al artículo 9, con las autoridades competentes de otros Estados miembros de la Unión Europea, así como con el grupo de cooperación y la red de CSIRT.

Artículo 14. *Cooperación con otras autoridades con competencias en seguridad de la información y con las autoridades sectoriales.*

1. Las autoridades competentes, los CSIRT de referencia y el punto de contacto único consultarán, cuando proceda, con los órganos con competencias en materia de seguridad nacional, seguridad pública, seguridad ciudadana y protección de datos de carácter personal y colaborarán con ellas en el ejercicio de sus respectivas funciones.
2. Consultarán así mismo, cuando proceda, con los órganos con competencias por razón de la materia en cada uno de los sectores incluidos en el ámbito de aplicación de este real decreto-ley, y colaborarán con ellos en el ejercicio de sus funciones.
3. Cuando los incidentes notificados presenten caracteres de delito, las autoridades competentes y los CSIRT de referencia darán cuenta de ello, a través de la Oficina de Coordinación Cibernética del Ministerio del Interior, al Ministerio Fiscal a los efectos oportunos, trasladándole al tiempo cuanta información posean en relación con ello.

Artículo 15. *Confidencialidad de la información sensible.*

Sin perjuicio de lo dispuesto en el artículo 5, las autoridades competentes, los CSIRT de referencia y el punto de contacto único preservarán, como corresponda en Derecho, la seguridad y los intereses comerciales de los operadores de servicios esenciales y proveedores de servicios digitales, así como la confidencialidad de la información que recaben de éstos en el ejercicio de las funciones que les encomienda el presente real decreto-ley.
Cuando ello sea necesario, el intercambio de información sensible se limitará a aquella que sea pertinente y proporcionada para la finalidad de dicho intercambio.

TÍTULO IV

Obligaciones de seguridad

Artículo 16. *Obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales.*

1. Los operadores de servicios esenciales y los proveedores de servicios digitales deberán adoptar medidas técnicas y de organización, adecuadas y proporcionadas, para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información utilizados en la prestación de los servicios sujetos a este real decreto-ley.
Sin perjuicio de su deber de notificar incidentes conforme al título V, deberán tomar medidas adecuadas para prevenir y reducir al mínimo el impacto de los incidentes que les afecten.
2. El desarrollo reglamentario de este real decreto-ley preverá las medidas necesarias para el cumplimiento de lo preceptuado en el apartado anterior por parte de los operadores de servicios esenciales.
3. Los operadores de servicios esenciales designarán y comunicarán a la autoridad competente, en el plazo que reglamentariamente se establezca, la persona, unidad u órgano

colegiado responsable de la seguridad de la información, como punto de contacto y de coordinación técnica con aquella.

Sus funciones específicas serán las previstas reglamentariamente.

4. Las autoridades competentes podrán establecer mediante Orden ministerial obligaciones específicas para garantizar la seguridad de las redes y sistemas de información empleados por los operadores de servicios esenciales. Así mismo, podrán dictar instrucciones técnicas y guías orientativas para detallar el contenido de dichas órdenes.

Al elaborar las disposiciones reglamentarias, instrucciones y guías, tendrán en cuenta las obligaciones sectoriales, las directrices relevantes que se adopten en el grupo de cooperación y los requisitos en materia de seguridad de la información, a las que estuviera sometido el operador en virtud de otras normas, como la Ley 8/2011, de 28 de abril, y el Esquema Nacional de Seguridad, aprobado por el Real Decreto 3/2010, de 8 de enero.

5. Las autoridades competentes deberán coordinarse entre sí y con los diferentes órganos sectoriales con competencias por razón de la materia, en lo relativo al contenido y a la aplicación de las órdenes, instrucciones técnicas y guías orientativas que dicten en sus respectivos ámbitos de competencia, con objeto de evitar duplicidades en las obligaciones exigibles y facilitar su cumplimiento a los operadores de servicios esenciales.

6. Los proveedores de servicios digitales determinarán las medidas de seguridad que aplicarán, teniendo en cuenta, como mínimo, los avances técnicos y los siguientes aspectos:

a) La seguridad de los sistemas e instalaciones;
b) La gestión de incidentes;
c) La gestión de la continuidad de las actividades;
d) La supervisión, auditorías y pruebas;
e) El cumplimiento de las normas internacionales.

Los proveedores de servicios digitales atenderán igualmente a los actos de ejecución por los que la Comisión europea detalle los aspectos citados.

7. Los operadores de servicios esenciales y proveedores de servicios digitales que no siendo operadores críticos se encuentren comprendidos en el ámbito de aplicación de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público que utilizan servicios ofrecidos por proveedores de servicios digitales, en particular servicios de computación en nube, podrán exigir a los proveedores de tales servicios medidas de seguridad adicionales, más estrictas que las que dichos proveedores han adoptado en cumplimiento de la legislación en materia de seguridad de las redes y sistemas de información. En particular, las citadas medidas podrán ser exigidas mediante obligaciones contractuales, previo informe preceptivo y vinculante del Centro Criptológico Nacional.

Artículo 17. *Normas técnicas.*

Las autoridades competentes promoverán la utilización de regulaciones, normas o especificaciones técnicas en materia de seguridad de las redes y sistemas de información elaboradas en el marco del Reglamento (UE) 1025/2012 del Parlamento Europeo y del Consejo de 25 de octubre de 2012 sobre la normalización europea.

En ausencia de dichas normas o especificaciones, promoverán la aplicación de las normas o recomendaciones internacionales aprobadas por los organismos internacionales de normalización, y, en su caso, de las normas y especificaciones técnicas aceptadas a nivel europeo o internacional que sean pertinentes en esta materia.

Artículo 18. *Sectores con normativa específica equivalente.*

Cuando una normativa nacional o comunitaria establezca para un sector obligaciones de seguridad de las redes y sistemas de información o de notificación de incidentes que tengan efectos, al menos, equivalentes a los de las obligaciones previstas en este real decreto-ley, prevalecerán aquellos requisitos y los mecanismos de supervisión correspondientes.

Ello no afectará al deber de cooperación entre autoridades competentes, a la coordinación ejercida por el Consejo de Seguridad Nacional ni, en la medida en que no sea incompatible con la legislación sectorial, a la aplicación del título V sobre notificación de incidentes.

TÍTULO V

Notificación de incidentes

Artículo 19. *Obligación de notificar.*

1. Los operadores de servicios esenciales notificarán a la autoridad competente, a través del CSIRT de referencia, los incidentes que puedan tener efectos perturbadores significativos en dichos servicios.

Las notificaciones podrán referirse también, conforme se determine reglamentariamente, a los sucesos o incidencias que puedan afectar a las redes y sistemas de información empleados para la prestación de los servicios esenciales, pero que aún no hayan tenido un efecto adverso real sobre aquéllos.

2. Así mismo, los proveedores de servicios digitales notificarán a la autoridad competente, a través del CSIRT de referencia, los incidentes que tengan efectos perturbadores significativos en dichos servicios.

La obligación de la notificación del incidente únicamente se aplicará cuando el proveedor de servicios digitales tenga acceso a la información necesaria para valorar el impacto de un incidente.

3. Las notificaciones tanto de operadores de servicios esenciales como de proveedores de servicios digitales se referirán a los incidentes que afecten a las redes y sistemas de información empleados en la prestación de los servicios indicados, tanto si se trata de redes y servicios propios como si lo son de proveedores externos, incluso si éstos son proveedores de servicios digitales sometidos a este real decreto-ley.

4. Las autoridades competentes y los CSIRT de referencia utilizarán una plataforma común para facilitar y automatizar los procesos de notificación, comunicación e información sobre incidentes.

5. El desarrollo reglamentario de este real decreto-ley preverá las medidas necesarias para el cumplimiento de lo preceptuado en este artículo por parte de los operadores de servicios esenciales. Las autoridades competentes podrán establecer, mediante Orden ministerial, obligaciones específicas de notificación por los operadores de servicios esenciales. Así mismo, podrán dictar instrucciones técnicas y guías orientativas para detallar el contenido de dichas órdenes.

Al elaborar las disposiciones reglamentarias, instrucciones y guías, se tendrán en cuenta las obligaciones sectoriales, las directrices relevantes que se adopten en el grupo de cooperación y los requisitos en materia de notificación de incidentes a los que estuviera sometido el operador en virtud de otras normas, como la Ley 8/2011, de 28 de abril, y el Esquema Nacional de Seguridad, aprobado por el Real Decreto 3/2010, de 8 de enero.

6. La obligación de notificación de incidentes prevista en los apartados anteriores no obsta al cumplimiento de los deberes legales de denuncia de aquellos hechos que revistan caracteres de delito ante las autoridades competentes, de acuerdo con lo dispuesto en los artículos 259 y siguientes de la Ley de Enjuiciamiento Criminal y teniendo en cuenta lo previsto en el artículo 14.3 de este real decreto-ley.

Artículo 20. *Protección del notificante.*

1. Las notificaciones consideradas en este título no sujetarán a la entidad que las efectúe a una mayor responsabilidad.

2. Los empleados y el personal que, por cualquier tipo de relación laboral o mercantil, participen en la prestación de los servicios esenciales o digitales, que informen sobre incidentes no podrán sufrir consecuencias adversas en su puesto de trabajo o con la empresa, salvo en los supuestos en que se acredite mala fe en su actuación.

Se entenderán nulas y sin efecto legal las decisiones del empleador tomadas en perjuicio o detrimento de los derechos laborales de los trabajadores que hayan actuado conforme a este apartado.

Artículo 21. *Factores para determinar la importancia de los efectos de un incidente.*

1. A los efectos de las notificaciones a las que se refiere el artículo 19.1, primer párrafo, la importancia de un incidente se determinará teniendo en cuenta, como mínimo, los siguientes factores:

a) El número de usuarios afectados por la perturbación del servicio esencial.
b) La duración del incidente.
c) La extensión o áreas geográficas afectadas por el incidente.
d) El grado de perturbación del funcionamiento del servicio.
e) El alcance del impacto en actividades económicas y sociales cruciales.
f) La importancia de los sistemas afectados o de la información afectada por el incidente para la prestación del servicio esencial.
g) El daño a la reputación.

2. En las notificaciones a las que se refiere el artículo 19.2, la importancia de un incidente se determinará conforme a lo que establezcan los actos de ejecución previstos en los apartados 8 y 9 del artículo 16 de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016.

Artículo 22. *Notificación inicial, notificaciones intermedias y notificación final.*

1. Los operadores de servicios esenciales deberán realizar una primera notificación de los incidentes a los que se refiere el artículo 19.1 sin dilación indebida.

La notificación incluirá, entre otros datos, información que permita determinar cualquier efecto transfronterizo del incidente.

2. Los operadores de servicios esenciales efectuarán las notificaciones intermedias que sean precisas para actualizar la información incorporada a la notificación inicial e informar sobre la evolución del incidente, mientras éste no esté resuelto.

3. Los operadores de servicios esenciales enviarán una notificación final del incidente tras su resolución.

Un incidente se considerará resuelto cuando se hayan restablecido las redes y sistemas de información afectados y el servicio opere con normalidad.

Artículo 23. *Flexibilidad en la observancia de los plazos para la notificación.*

Los operadores de servicios esenciales y los proveedores de servicios digitales podrán omitir, en las comunicaciones que realicen sobre los incidentes que les afecten, la información de la que aún no dispongan relativa a su repercusión sobre servicios esenciales u otros servicios que dependan de ellos para su prestación, u otra información de la que no dispongan. Tan pronto como conozcan dicha información deberán remitirla a la autoridad competente.

Si, transcurrido un tiempo prudencial desde la notificación inicial del incidente, el operador de servicios esenciales o el proveedor de servicios digitales no hubiera podido reunir la información pertinente, enviará a la autoridad competente, sin demora, un informe justificativo de las actuaciones realizadas para reunir la información y de los motivos por los que no ha sido posible obtenerla.

Artículo 24. *Incidentes que afecten a servicios digitales.*

Los operadores de servicios esenciales y los proveedores de servicios digitales sometidos a este real decreto-ley, así como cualquier otra parte interesada, que tengan noticia de incidentes que afecten de modo significativo a servicios digitales ofrecidos en España por proveedores establecidos en otros Estados miembros de la Unión Europea, podrán notificarlo a la autoridad competente aportando la información pertinente, al objeto de facilitar la cooperación con el Estado miembro en el que estuviese establecido el citado proveedor.

Del mismo modo, si tienen noticia de que dichos proveedores han incumplido los requisitos de seguridad o de notificación de incidentes ocurridos en España que les son aplicables, podrán notificarlo a la autoridad competente aportando la información pertinente.

Artículo 25. *Tramitación de incidentes con impacto transfronterizo.*

1. Cuando las autoridades competentes o los CSIRT de referencia tengan noticia de incidentes que pueden afectar a otros Estados miembros de la Unión Europea, informarán a través del punto de contacto único a los Estados miembros afectados, precisando si el incidente puede tener efectos perturbadores significativos para los servicios esenciales prestados en dichos Estados.

2. Cuando a través de dicho punto de contacto se reciba información sobre incidentes notificados en otros países de la Unión Europea que puedan tener efectos perturbadores significativos para los servicios esenciales prestados en España, se remitirá la información relevante a la autoridad competente y al CSIRT de referencia, para que adopten las medidas pertinentes en el ejercicio de sus funciones respectivas.

3. Las actuaciones consideradas en los apartados anteriores se entienden sin perjuicio de los intercambios de información que las autoridades competentes o los CSIRT de referencia puedan realizar de modo directo con sus homólogos de otros Estados miembros de la Unión Europea en relación con aquellos incidentes que puedan resultar de interés mutuo.

Artículo 26. *Información al público.*

1. La autoridad competente podrá exigir a los operadores de servicios esenciales o a los proveedores de servicios digitales que informen al público o a terceros potencialmente interesados sobre los incidentes cuando su conocimiento sea necesario para evitar nuevos incidentes o gestionar uno que ya se haya producido, o cuando la divulgación de un incidente redunde en beneficio del interés público.

2. La autoridad competente también podrá decidir informar de modo directo al público o a terceros sobre el incidente.

En estos casos la autoridad competente consultará y se coordinará con el operador de servicios esenciales o el proveedor de servicios digitales antes de informar al público.

Artículo 27. *Información anual al punto de contacto único y al grupo de cooperación.*

1. Las autoridades competentes transmitirán al punto de contacto único un informe anual sobre el número y tipo de incidentes comunicados, sus efectos en los servicios prestados o en otros servicios y su carácter nacional o transfronterizo dentro de la Unión Europea.

Las autoridades competentes elaborarán el informe siguiendo las instrucciones que dicte el punto de contacto único teniendo en cuenta las indicaciones del grupo de cooperación respecto al formato y contenido de la información a transmitir.

2. El punto de contacto único remitirá al grupo de cooperación antes del 9 de agosto de cada año un informe anual resumido sobre las notificaciones recibidas, y lo remitirá ulteriormente a las autoridades competentes y a los CSIRT de referencia, para su conocimiento.

Artículo 28. *Obligación de resolver los incidentes, de información y de colaboración mutua.*

1. Los operadores de servicios esenciales y los proveedores de servicios digitales tienen la obligación de resolver los incidentes de seguridad que les afecten, y de solicitar ayuda especializada, incluida la del CSIRT de referencia, cuando no puedan resolver por sí mismos los incidentes.

En tales casos deberán atender a las indicaciones que reciban del CSIRT de referencia para resolver el incidente, mitigar sus efectos y reponer los sistemas afectados.

2. Los operadores de servicios esenciales y los proveedores de servicios digitales han de suministrar al CSIRT de referencia y a la autoridad competente toda la información que se les requiera para el desempeño de las funciones que les encomienda el presente real decreto-ley.

En particular, podrá requerirse información adicional a los operadores de servicios esenciales y a los proveedores de servicios digitales para analizar la naturaleza, causas y efectos de los incidentes notificados, y para elaborar estadísticas y reunir los datos necesarios para elaborar los informes anuales considerados en el artículo 27.

Cuando las circunstancias lo permitan, la autoridad competente o el CSIRT de referencia proporcionarán a los operadores de servicios esenciales o a los proveedores de servicios digitales afectados por incidentes la información derivada de su seguimiento que pueda serles relevante, en particular, para resolver el incidente.

Artículo 29. *Cooperación en lo relativo a los incidentes que afecten a datos personales.*

Las autoridades competentes y los CSIRT de referencia cooperarán estrechamente con la Agencia Española de Protección de Datos para hacer frente a los incidentes que den lugar a violaciones de datos personales.

Las autoridades competentes y los CSIRT de referencia comunicarán sin dilación a la Agencia Española de Protección de Datos los incidentes que puedan suponer una vulneración de datos personales y la mantendrán informada sobre la evolución de tales incidentes.

Artículo 30. *Autorización para la cesión de datos personales.*

Si la notificación de incidentes o su gestión, análisis o resolución requiriera comunicar datos personales, su tratamiento se restringirá a los que sean estrictamente adecuados, pertinentes y limitados a lo necesario en relación con la finalidad, de las indicadas, que se persiga en cada caso.

Su cesión para estos fines se entenderá autorizada en los siguientes casos:

a) De los operadores de servicios esenciales y los proveedores de servicios digitales a las autoridades competentes, a través de los CSIRT de referencia.

b) Entre los CSIRT de referencia y las autoridades competentes, y viceversa.

c) Entre los CSIRT de referencia, y entre éstos y los CSIRT designados en otros Estados miembros de la Unión Europea.

d) Entre los CSIRT de referencia y otros CSIRT nacionales o internacionales.

e) Entre el punto de contacto único y los puntos de contacto únicos de otros Estados miembros de la Unión Europea.

Artículo 31. *Notificaciones voluntarias.*

1. Los operadores de servicios esenciales y los proveedores de servicios digitales podrán notificar los incidentes para los que no se establezca una obligación de notificación.

Así mismo, las entidades que presten servicios esenciales y no hayan sido identificadas como operadores de servicios esenciales y que no sean proveedores de servicios digitales podrán notificar los incidentes que afecten a dichos servicios.

Estas notificaciones obligan a la entidad que las efectúe a resolver el incidente de acuerdo con lo establecido en el artículo 28.

2. Las notificaciones a las que se refiere el apartado anterior se regirán por lo dispuesto en este título, y se informará sobre ellas al punto de contacto único en el informe anual previsto en el artículo 27.1.

3. Las notificaciones obligatorias gozarán de prioridad sobre las voluntarias a los efectos de su gestión por los CSIRT y por las autoridades competentes.

TÍTULO VI

Supervisión

Artículo 32. *Supervisión de los operadores de servicios esenciales.*

1. Las autoridades competentes podrán requerir a los operadores de servicios esenciales para que les proporcionen toda la información necesaria para evaluar la seguridad de las redes y sistemas de información, incluida la documentación sobre políticas de seguridad.

Podrán requerirles información sobre la aplicación efectiva de su política de seguridad, así como auditar o exigir al operador que someta la seguridad de sus redes y sistemas de información a una auditoría por una entidad externa, solvente e independiente.

2. A la vista de la información recabada, la autoridad competente podrá requerir al operador que subsane las deficiencias detectadas e indicarle cómo debe hacerlo.

Artículo 33. *Supervisión de los proveedores de servicios digitales.*

1. La autoridad competente para la supervisión de los servicios digitales sólo inspeccionará el cumplimiento de las obligaciones derivadas de este real decreto-ley cuando tenga noticia de algún incumplimiento, incluyendo por petición razonada de otros órganos o denuncia.

En tal caso, la autoridad competente podrá requerir al proveedor de servicios digitales para que le proporcione toda la información necesaria para evaluar la seguridad de sus redes y sistemas de información, incluida la documentación sobre políticas de seguridad, y para que subsane las deficiencias detectadas.

2. Cuando la autoridad competente tenga noticia de incidentes que perturben de modo significativo a servicios digitales ofrecidos en otros Estados miembros por proveedores establecidos en España, adoptará las medidas de supervisión pertinentes.

A estos efectos, tendrá especialmente en cuenta la información facilitada por las autoridades competentes de otros Estados miembros.

Artículo 34. *Cooperación transfronteriza.*

1. La supervisión se llevará a cabo, cuando proceda, en cooperación con las autoridades competentes de los Estados miembros en los que se ubiquen las redes y sistemas de información empleados para la prestación del servicio, o en que esté establecido el operador de servicios esenciales, el proveedor de servicios digitales o su representante.

2. Las autoridades competentes colaborarán con las autoridades competentes de otros Estados miembros cuando éstas requieran su cooperación en la supervisión y adopción de medidas por operadores de servicios esenciales y proveedores de servicios digitales en relación con las redes y sistemas de información ubicados en España, así como respecto a los proveedores de servicios digitales establecidos en España o cuyo representante en la Unión Europea tenga su residencia o domicilio social en España.

TÍTULO VII

Régimen sancionador

Artículo 35. *Responsables.*

Serán responsables los operadores de servicios esenciales y los proveedores de servicios digitales comprendidos en el ámbito de aplicación de este real decreto-ley.

Artículo 36. *Infracciones.*

1. Las infracciones de los preceptos de este real decreto-ley se clasifican en muy graves, graves y leves.

2. Son infracciones muy graves:

a) La falta de adopción de medidas para subsanar las deficiencias detectadas, de acuerdo con lo dispuesto en los artículos 32.2 o 33.1, cuando éstas le hayan hecho vulnerable a un incidente con efectos perturbadores significativos en el servicio y el operador de servicios esenciales o el proveedor de servicios digitales no hubiera atendido los requerimientos dictados por la autoridad competente con anterioridad a la producción del incidente.

b) El incumplimiento reiterado de la obligación de notificar incidentes con efectos perturbadores significativos en el servicio. Se considerará que es reiterado a partir del segundo incumplimiento.

c) No tomar las medidas necesarias para resolver los incidentes con arreglo a lo dispuesto en el artículo 28.1 cuando éstos tengan un efecto perturbador significativo en la prestación servicios esenciales o de servicios digitales en España o en otros Estados miembros.

3. Son infracciones graves:

a) El incumplimiento de las disposiciones reglamentarias o de las instrucciones técnicas de seguridad dictadas por la autoridad competente referidas a las precauciones mínimas que los operadores de servicios esenciales han de adoptar para garantizar la seguridad de las redes y sistemas de información.

b) La falta de adopción de medidas para subsanar las deficiencias detectadas en respuesta a un requerimiento dictado de acuerdo con los artículos 32.2 o 33.1, cuando ese sea el tercer requerimiento desatendido que se dicta en los cinco últimos años.

c) El incumplimiento de la obligación de notificar incidentes con efectos perturbadores significativos en el servicio.

d) La demostración de una notoria falta de interés en la resolución de incidentes con efectos perturbadores significativos notificados cuando dé lugar a una mayor degradación del servicio.

e) Proporcionar información falsa o engañosa al público sobre los estándares que cumple o las certificaciones de seguridad que mantiene en vigor.

f) Poner obstáculos a la realización de auditorías por la autoridad competente.

4. Son infracciones leves:

a) El incumplimiento de las disposiciones reglamentarias o de las instrucciones técnicas de seguridad dictadas por la autoridad competente al amparo de este real decreto-ley, cuando no suponga una infracción grave.

b) La falta de adopción de medidas para corregir las deficiencias detectadas en respuesta a un requerimiento de subsanación dictado de acuerdo con los artículos 32.2 o 33.1.

c) No facilitar la información que sea requerida por las autoridades competentes sobre sus políticas de seguridad, o proporcionar información incompleta o tardía sin justificación.

d) No someterse a una auditoría de seguridad según lo ordenado por la autoridad competente.

e) No proporcionar al CSIRT de referencia o a la autoridad competente la información que soliciten en virtud del artículo 28.2.

f) La falta de notificación de los sucesos o incidencias para los que, aunque no hayan tenido un efecto adverso real sobre los servicios, exista obligación de notificación en virtud del párrafo segundo del artículo 19.2.

g) No completar la información que debe reunir la notificación de incidentes teniendo en cuenta lo dispuesto en el artículo 23, o no remitir el informe justificativo sobre la imposibilidad de reunir la información previsto en dicho artículo.

h) No seguir las indicaciones que reciba del CSIRT de referencia para resolver un incidente, de acuerdo con el artículo 28.

Artículo 37. *Sanciones.*

1. Por la comisión de las infracciones recogidas en el artículo anterior, se impondrán las siguientes sanciones:

a) Por la comisión de infracciones muy graves, multa de 500.001 hasta 1.000.000 euros.
b) Por la comisión de infracciones graves, multa de 100.001 hasta 500.000 euros.
c) Por la comisión de infracciones leves, amonestación o multa hasta 100.000 euros.

2. Las sanciones firmes en vía administrativa por infracciones muy graves y graves podrán ser publicadas, a costa del sancionado, en el «Boletín Oficial del Estado» y en el sitio de Internet de la autoridad competente, en atención a los hechos concurrentes y de conformidad con el artículo siguiente.

Artículo 38. *Graduación de la cuantía de las sanciones.*

El órgano sancionador establecerá la sanción teniendo en cuenta los siguientes criterios:

a) El grado de culpabilidad o la existencia de intencionalidad.
b) La continuidad o persistencia en la conducta infractora.
c) La naturaleza y cuantía de los perjuicios causados.

d) La reincidencia, por comisión en el último año de más de una infracción de la misma naturaleza, cuando así haya sido declarado por resolución firme en vía administrativa.
e) El número de usuarios afectados.
f) El volumen de facturación del responsable.
g) La utilización por el responsable de programas de recompensa por el descubrimiento de vulnerabilidades en sus redes y sistemas de información.
h) Las acciones realizadas por el responsable para paliar los efectos o consecuencias de la infracción.

Artículo 39. *Proporcionalidad de sanciones.*

1. El órgano sancionador podrá establecer la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate, en los siguientes supuestos:

a) Cuando se aprecie una cualificada disminución de la culpabilidad del imputado como consecuencia de la concurrencia significativa de varios de los criterios enunciados en el artículo 38.
b) Cuando la entidad infractora haya regularizado la situación irregular de forma diligente.
c) Cuando el infractor haya reconocido espontáneamente su culpabilidad.

2. Los órganos con competencia sancionadora, atendida la naturaleza de los hechos y la concurrencia significativa de los criterios establecidos en el apartado anterior, podrán no acordar el inicio del procedimiento sancionador y, en su lugar, apercibir al sujeto responsable a fin de que, en el plazo que el órgano sancionador determine, acredite la adopción de las medidas correctoras que, en cada caso, resulten pertinentes, siempre que concurran los siguientes presupuestos:

a) Que los hechos fuesen constitutivos de infracción leve o grave conforme a lo dispuesto en este real decreto-ley.
b) Que el órgano competente no hubiese sancionado o apercibido al infractor en los dos años previos como consecuencia de la comisión de infracciones previstas en este real decreto-ley.

Si el apercibimiento no fuera atendido en el plazo que el órgano sancionador hubiera determinado, procederá la apertura del correspondiente procedimiento sancionador por dicho incumplimiento.
3. No podrán ser objeto de apercibimiento las infracciones leves descritas en el artículo 36.4 c), d) y e) y la infracción grave prevista en el artículo 36.3 e).

Artículo 40. *Infracciones de las Administraciones públicas.*

1. Cuando las infracciones a que se refiere el artículo 36 fuesen cometidas por órganos o entidades de las Administraciones Públicas, el órgano sancionador dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Esta resolución se notificará al órgano o entidad infractora y a los afectados, si los hubiera.
Además de lo anterior, el órgano sancionador podrá proponer también la iniciación de actuaciones disciplinarias, si procedieran.
2. Se deberán comunicar al órgano sancionador las resoluciones que recaigan en relación con las medidas y actuaciones a que se refiere el apartado anterior.

Artículo 41. *Competencia sancionadora.*

1. La imposición de sanciones corresponderá, en el caso de infracciones muy graves, al Ministro competente en virtud de lo dispuesto en el artículo 9, y en el caso de infracciones graves y leves al órgano de la autoridad competente que se determine mediante el reglamento de desarrollo de este real decreto-ley.
2. La potestad sancionadora se ejercerá con arreglo a los principios y al procedimiento previstos en las Leyes 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de

las Administraciones Públicas, y 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

3. El ejercicio de la potestad sancionadora se sujetará al procedimiento aplicable, con carácter general, a la actuación de las Administraciones públicas. No obstante, el plazo máximo de duración del procedimiento será de un año y el plazo de alegaciones no tendrá una duración inferior a un mes.

Artículo 42. *Concurrencia de infracciones.*

1. No procederá la imposición de sanciones según lo previsto en este real decreto-ley cuando los hechos constitutivos de infracción lo sean también de otra tipificada en la normativa sectorial a la que esté sujeto el prestador del servicio y exista identidad del bien jurídico protegido.

2. Cuando, como consecuencia de una actuación sancionadora, se tuviera conocimiento de hechos que pudieran ser constitutivos de infracciones tipificadas en otras leyes, se dará cuenta de los mismos a los órganos u organismos competentes para su supervisión y sanción.

Disposición adicional primera. *Relación inicial de servicios esenciales y operadores de servicios esenciales.*

La Comisión Nacional para la Protección de las Infraestructuras Críticas aprobará una primera lista de servicios esenciales dentro de los sectores incluidos en el ámbito de aplicación de este real decreto-ley e identificará a los operadores que los presten que deban sujetarse a este real decreto-ley en el siguiente orden:

a) Antes del 9 de noviembre de 2018: los servicios esenciales y los operadores correspondientes a los sectores estratégicos energía, transporte, salud, sistema financiero, agua, e infraestructuras digitales.

b) Antes del 9 de noviembre de 2019: los servicios esenciales y los operadores correspondientes al resto de los sectores estratégicos recogidos en el anexo de la Ley 8/2011, de 28 de abril.

Disposición adicional segunda. *Comunicaciones electrónicas y servicios de confianza.*

La aplicación de este real decreto-ley a los operadores de redes y servicios de comunicaciones electrónicas y de servicios electrónicos de confianza que sean designados como operadores críticos en virtud de la Ley 8/2011, de 28 de abril, no obstará a la aplicación de su normativa específica en materia de seguridad.

El Ministerio de Economía y Empresa, como órgano competente para la aplicación de dicha normativa, y el Ministerio del Interior actuarán de manera coordinada en el establecimiento de obligaciones que recaigan sobre los operadores críticos. Así mismo, mantendrán un intercambio fluido de información sobre incidentes que les afecten.

Disposición adicional tercera. *Notificación de violaciones de seguridad de los datos personales a través de la plataforma común prevista en este real decreto-ley.*

La plataforma común para la notificación de incidentes prevista en este real decreto-ley podrá ser empleada para la notificación de vulneraciones de la seguridad de datos personales según el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, en los términos que acuerden la Agencia Española de Protección de Datos y los órganos que gestionen dicha plataforma.

Disposición adicional cuarta. *Proveedores de servicios digitales ya existentes.*

Los proveedores de servicios digitales que ya vinieran prestando servicios deberán comunicar su actividad a la Secretaría de Estado para el Avance Digital del Ministerio de Economía y Empresa, en el plazo de tres meses desde la entrada en vigor de este real decreto-ley.

Disposición final primera. *Título competencial.*

Este real decreto-ley se dicta en virtud de las competencias exclusivas atribuidas al Estado en materia de régimen general de telecomunicaciones y seguridad pública, por el artículo 149.1.21.ª y 29.ª de la Constitución.

Disposición final segunda. *Incorporación del Derecho de la Unión Europea.*

Este real decreto-ley incorpora al ordenamiento jurídico interno la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

Disposición final tercera. *Habilitación para el desarrollo reglamentario.*

Se habilita al Gobierno para desarrollar reglamentariamente lo previsto en este real decreto-ley sin perjuicio de la competencia de los Ministros para fijar las obligaciones específicas mediante Orden Ministerial en los supuestos previstos en el articulado de esta norma.

Disposición final cuarta. *Entrada en vigor.*

El presente real decreto-ley entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

§ 12

Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información

Ministerio de la Presidencia, Relaciones con las Cortes y Memoria Democrática
«BOE» núm. 24, de 28 de enero de 2021
Última modificación: sin modificaciones
Referencia: BOE-A-2021-1192

En el ámbito europeo, con el objetivo de dar una respuesta efectiva a los problemas de seguridad de las redes y sistemas de información, se aprobó la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, conocida como la Directiva NIS (Security of Network and Information Systems). Esta norma parte de un enfoque global de la seguridad de las redes y sistemas de información en la Unión Europea, integrando requisitos mínimos comunes en materia de desarrollo de capacidades y planificación, intercambio de información, cooperación y requisitos comunes de seguridad para los operadores de servicios esenciales y los proveedores de servicios digitales.

La transposición de la citada Directiva NIS al ordenamiento jurídico español se llevó a cabo mediante el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. Esta norma legal regula la seguridad de las redes y sistemas de información utilizados para la provisión de los servicios esenciales y los servicios digitales, estableciendo mecanismos que, con una perspectiva integral, permiten mejorar la protección frente a las amenazas que afectan a las redes y sistemas de información, y fijando un marco institucional de cooperación que facilita la coordinación de las actuaciones realizadas en esta materia tanto a nivel nacional como con los países de nuestro entorno, en particular, dentro de la Unión Europea.

El Real Decreto-ley 12/2018, de 7 de septiembre, habilita al Gobierno, en su disposición final tercera, para su desarrollo reglamentario. Con esa cobertura legal, y en cumplimiento del citado mandato y lo previsto en sus artículos 9.1 a), 11.1 a), 11.2, 16.2, 16.3, 19.1 y 19.5, este real decreto tiene por finalidad desarrollar el Real Decreto-ley 12/2018, de 7 de septiembre, en lo relativo al marco estratégico e institucional de seguridad de las redes y sistemas de información al cumplimiento de las obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales y a la gestión de incidentes de seguridad.

El real decreto, en su artículo 3, pormenoriza la designación de autoridades competentes en materia de seguridad de las redes y sistemas de información prevista en el artículo 9.1.a) 2.º del Real Decreto-ley 12/2018, de 7 de septiembre. Es oportuno mencionar, en relación con la seguridad en el sector de la alimentación, la participación de la Agencia Española de Seguridad Alimentaria y Nutrición, dependiente del Ministerio de Consumo. Adicionalmente,

y de conformidad con el artículo 11 del Real Decreto-ley 12/2018, de 7 de septiembre, el real decreto desarrolla los supuestos de cooperación y coordinación entre los equipos de respuesta a incidentes de seguridad informática (CSIRT) de referencia, y de estos con las autoridades competentes, que se instrumentan a través de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes (artículo 4).

Con relación a la figura del punto de contacto único (artículo 5) que consagra la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, se desarrollan sus funciones de enlace para garantizar la cooperación transfronteriza con las autoridades competentes de otros Estados miembros de la Unión Europea, así como con el grupo de cooperación y la red de CSIRT.

Por otra parte, el artículo 6 de este real decreto desarrolla las previsiones del artículo 16.2 del Real Decreto-ley 12/2018, de 7 de septiembre, sobre las medidas necesarias para el cumplimiento de las obligaciones de seguridad por parte de los operadores de servicios esenciales, que habrán de concretarse en una declaración de aplicabilidad de medidas de seguridad suscrita por el responsable de seguridad de la información del operador, cuyas funciones también se desarrollan en el artículo 7 de este real decreto. El plazo para la designación del responsable de la seguridad se establece en cumplimiento de la habilitación recogida en el artículo 16.3 del Real Decreto-ley 12/2018, de 7 de septiembre.

Por lo que se refiere a la notificación de incidentes, el real decreto, en sus artículos 8 y 9, desarrolla las obligaciones de notificación por parte de los operadores de servicios esenciales de los incidentes que puedan tener efectos perturbadores significativos en dichos servicios, así como de los incidentes que puedan afectar a las redes y sistemas de información empleados para la prestación de los servicios esenciales aun cuando no hayan tenido un efecto adverso real sobre aquellos, por referencia a los niveles de impacto y peligrosidad, según sea el caso, previstos en la Instrucción nacional de notificación y gestión de ciberincidentes que se contiene en el anexo.

El procedimiento de notificación de incidentes se articula a través de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes (artículos 10 y 11), a fin de permitir el intercambio de información entre los operadores de servicios esenciales y proveedores de servicios digitales, las autoridades competentes y los CSIRT de referencia, garantizando la confidencialidad, integridad y disponibilidad de la información (artículos 12 a 14).

Por último, en materia de supervisión de requisitos de seguridad, el real decreto desarrolla en su artículo 15 la obligación de colaboración de los operadores de servicios esenciales y los proveedores de servicios digitales con las autoridades competentes, que podrán requerir, asimismo, la colaboración de los CSIRT de referencia para el ejercicio de su función de supervisión.

En las disposiciones adicionales de este real decreto se recoge, entre otras materias, el régimen jurídico aplicable al Banco de España teniendo en cuenta su especial configuración jurídica como entidad de Derecho público con personalidad jurídica propia y plena capacidad pública y privada, que en el desarrollo de su actividad y para el cumplimiento de sus fines actúa con autonomía respecto a la Administración General del Estado, y como parte integrante del Sistema Europeo de Bancos Centrales (SEBC) y del Mecanismo Único de Supervisión (MUS). Esta especial configuración jurídica supone que el marco de seguridad de las redes y sistemas de información resulte de aplicación en la medida en que no interfiera con la naturaleza, funciones e independencia del Banco de España.

Este real decreto se adecúa a los principios de buena regulación establecidos en el artículo 129 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. Responde, en primer lugar, a los principios de necesidad y eficacia, en tanto que la norma es necesaria para llevar a cabo el desarrollo reglamentario del Real Decreto-ley 12/2018, de 7 de septiembre, que transpone la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016 y, en concreto, para establecer el marco estratégico e institucional de seguridad de las redes y sistemas de información, las obligaciones de seguridad y la gestión de incidentes, siendo el instrumento más idóneo para la consecución de este objetivo. En segundo término, la norma cumple con el principio de proporcionalidad, al no existir otras medidas menos gravosas para los operadores de servicios esenciales y proveedores de servicios digitales destinadas a cumplir

la obligación de adoptar medidas técnicas y de organización para gestionar los riesgos para la seguridad de sus redes y sistemas de información, así como de notificar los incidentes que tengan efectos perturbadores significativos en los servicios que prestan. Asimismo, este real decreto cumple con el principio de seguridad jurídica, resultando el proyecto conforme a la directiva europea de la que trae causa, así como con la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas y su normativa de desarrollo, la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, y la normativa comunitaria y nacional en materia de protección de datos. Se ha cumplido igualmente con el principio de transparencia, al haber sometido el proyecto de real decreto al trámite de audiencia, definiéndose claramente los objetivos de la iniciativa normativa y su justificación. Por último, este real decreto resulta conforme con el principio de eficiencia, dado que no se establecen cargas adicionales a las contempladas en el real decreto-ley que desarrolla.

En la elaboración de este real decreto se ha solicitado informe de todos los departamentos ministeriales, así como de la Agencia Española de Protección de Datos, de la Comisión Nacional de los Mercados y de la Competencia, de la Comisión Nacional del Mercado de Valores, del Consejo de Seguridad Nuclear, y del Banco de España. Adicionalmente, se ha solicitado informe a todas las comunidades autónomas y se ha dado audiencia a las organizaciones representativas de los sectores afectados.

En su virtud, a propuesta conjunta de la Vicepresidenta Tercera del Gobierno y Ministra de Asuntos Económicos y Transformación Digital, de la Ministra de Defensa, del Ministro del Interior y de la Vicepresidenta Primera del Gobierno y Ministra de la Presidencia, Relaciones con las Cortes y Memoria Democrática, con la aprobación previa de la Ministra de Política Territorial y Función Pública, de acuerdo con el Consejo de Estado, y previa deliberación del Consejo de Ministros en su reunión del día 26 de enero de 2021,

DISPONGO:

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

Este real decreto tiene por objeto desarrollar el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, en lo relativo al marco estratégico e institucional de seguridad de las redes y sistemas de información, la supervisión del cumplimiento de las obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales, y la gestión de incidentes de seguridad.

Artículo 2. *Ámbito de aplicación.*

1. De conformidad con el artículo 2 del Real Decreto-ley 12/2018, de 7 de septiembre, este real decreto se aplicará a la prestación de:

a) Los servicios esenciales dependientes de las redes y sistemas de información comprendidos en los sectores estratégicos definidos en el anexo de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

b) Los servicios digitales que sean mercados en línea, motores de búsqueda en línea y servicios de computación en nube.

2. Estarán sometidos a este real decreto:

a) Los operadores de servicios esenciales establecidos en España. Se entenderá que un operador de servicios esenciales está establecido en España cuando su residencia o domicilio social se encuentren en territorio español, siempre que estos coincidan con el lugar en que esté efectivamente centralizada la gestión administrativa y la dirección de sus negocios o actividades.

Así mismo, este real decreto será de aplicación a los servicios esenciales que los operadores residentes o domiciliados en otro Estado ofrezcan a través de un establecimiento permanente situado en España.

De conformidad con lo previsto en el apartado 1 del artículo 6 del Real Decreto-ley 12/2018, la identificación de los servicios esenciales y de los operadores que los presten se efectuará por los órganos y procedimientos previstos por la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, y su normativa de desarrollo, en particular el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

b) Los proveedores de servicios digitales que tengan su sede social en España y que constituya su establecimiento principal en la Unión Europea, así como los que, no estando establecidos en la Unión Europea, designen en España a su representante en la Unión para el cumplimiento de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

3. Este real decreto no se aplicará a:

a) Los operadores de redes y servicios de comunicaciones electrónicas y los prestadores de servicios electrónicos de confianza que no sean designados como operadores críticos en virtud de la Ley 8/2011, de 28 de abril.

b) Los proveedores de servicios digitales cuando se trate de microempresas o pequeñas empresas, de acuerdo con las definiciones recogidas en la Recomendación 2003/361/CE de la Comisión, de 6 de mayo de 2003, sobre la definición de microempresas, pequeñas y medianas empresas.

4. De conformidad con el artículo 18 del Real Decreto-ley 12/2018, de 7 de septiembre, cuando una normativa nacional o comunitaria establezca para un sector obligaciones de seguridad de las redes y sistemas de información o de notificación de incidentes que tengan efectos, al menos, equivalentes a los de las obligaciones previstas en el Real Decreto-ley 12/2018, de 7 de septiembre, prevalecerán aquellos requisitos y los mecanismos de supervisión correspondientes.

CAPÍTULO II

Marco estratégico e institucional

Artículo 3. *Autoridades competentes.*

Las autoridades competentes en materia de seguridad de las redes y sistemas de información serán, con carácter general, las establecidas en el artículo 9.1 del Real Decreto-ley 12/2018, de 7 de septiembre. En particular, son autoridades competentes para los operadores de servicios esenciales que no sean operadores críticos de acuerdo con la Ley 8/2011, de 28 de abril, y que no estén incluidos en el ámbito de aplicación de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, las siguientes:

a) Respecto al sector del transporte: el Ministerio de Transportes, Movilidad y Agenda Urbana, a través de la Secretaría de Estado de Transportes, Movilidad y Agenda Urbana.

b) Respecto al sector de la energía: el Ministerio para la Transición Ecológica y el Reto Demográfico, a través de la Secretaría de Estado de Energía.

c) Respecto al sector de las tecnologías de la información y las telecomunicaciones: el Ministerio de Asuntos Económicos y Transformación Digital, a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial y la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales.

d) Respecto al sector del sistema financiero:

1.º El Ministerio de Asuntos Económicos y Transformación Digital, a través de la Secretaría de Estado de Economía y Apoyo a la Empresa, en el ámbito de los seguros y fondos de pensiones.

2.º El Banco de España, para las entidades de crédito.

3.º La Comisión Nacional del Mercado de Valores, para las entidades que prestan servicios de inversión y las sociedades gestoras de instituciones de inversión colectiva.

e) Respecto al sector del espacio: el Ministerio de Defensa, a través de la Secretaría de Estado de Defensa.

f) Respecto al sector de la industria química: el Ministerio de Interior, a través de la Secretaría de Estado de Seguridad.

g) Respecto al sector de las instalaciones de investigación: el Ministerio de Ciencia e Innovación, a través de la Secretaría General de Investigación.

h) Respecto al sector de la salud: el Ministerio de Sanidad, a través de la Secretaría de Estado de Sanidad.

i) Respecto al sector del agua: el Ministerio para la Transición Ecológica y el Reto Demográfico, a través de la Secretaría de Estado de Medio Ambiente.

j) Respecto al sector de la alimentación:

1.º El Ministerio de Agricultura, Pesca y Alimentación, a través de la Secretaría General de Agricultura y Alimentación.

2.º El Ministerio de Sanidad, a través de la Secretaría de Estado de Sanidad.

3.º El Ministerio de Industria, Comercio y Turismo, a través de la Secretaría de Estado de Comercio.

4.º El Ministerio de Consumo, a través de la Agencia Española de Seguridad Alimentaria y Nutrición (AESAN).

k) Respecto al sector de la industria nuclear:

1.º El Ministerio para la Transición Ecológica y el Reto Demográfico, a través de la Secretaría de Estado de Energía.

2.º El Consejo de Seguridad Nuclear.

Artículo 4. *Cooperación y coordinación de los CSIRT de referencia.*

1. La cooperación entre los CSIRT de referencia, y entre estos y las autoridades competentes, se instrumentará a través de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes regulada en el artículo 11.

2. A efectos de la cooperación prevista en el artículo 11.1.a) 3.º del Real Decreto-ley 12/2018, de 7 de septiembre, se entenderá que son operadores con incidencia en la Defensa Nacional aquellos proveedores de servicios esenciales básicos para el funcionamiento del Ministerio de Defensa o para la operatividad de las Fuerzas Armadas que se establezcan, a propuesta del Ministerio de Defensa, por la Comisión Nacional para la Protección de las Infraestructuras Críticas.

La designación como operador con incidencia en la Defensa Nacional se llevará a cabo de conformidad con lo previsto en el Reglamento de protección de las infraestructuras críticas, aprobado por el Real Decreto 704/2011, de 20 de mayo. Así mismo, los CSIRT de referencia serán informados de la identidad de los operadores de servicios esenciales de su comunidad que sean designados operadores con incidencia en la Defensa Nacional.

El Ministerio de Defensa comunicará oportunamente a la Comisión Nacional para la Protección de las Infraestructuras Críticas las actualizaciones derivadas de cambios de operadores en la provisión de estos servicios, que activarán las correspondientes notificaciones de alta o baja como operadores con incidencia en la Defensa Nacional tanto a los propios operadores como a sus CSIRT de referencia.

Cuando un operador con incidencia en la Defensa Nacional sufra un incidente deberá analizar si, por su alcance, este pudiera tener impacto en el funcionamiento del Ministerio de Defensa o en la operatividad de las Fuerzas Armadas. En el caso de que así fuera, lo pondrá de inmediato en conocimiento de su CSIRT de referencia, quien informará al ESPDEF-CERT del Mando Conjunto del Ciberespacio a través de los canales establecidos. En estos casos, el ESPDEF-CERT del Mando Conjunto del Ciberespacio deberá ser oportunamente informado de la evolución de la gestión del incidente.

3. Los supuestos de especial gravedad a los que se refiere el artículo 11.2 párrafo primero del Real Decreto-ley 12/2018, de 7 de septiembre, en los que el CCN-CERT ejercerá la coordinación nacional de la respuesta técnica de los CSIRT, serán todos aquellos que,

atendiendo a la naturaleza de las notificaciones inicial o sucesivas del incidente recibidas por el CSIRT de referencia, posean un impacto o nivel de peligrosidad muy alta o crítica de acuerdo con lo establecido en el anexo, y exijan un nivel de coordinación técnica con los otros CSIRT de referencia superior al necesario en situaciones ordinarias.

El Consejo Nacional de Ciberseguridad será inmediatamente informado y podrá desactivar la coordinación prevista en este artículo, que únicamente podrá producirse cuando haya cesado la situación prevista en el párrafo anterior y que no afectará al proceso de notificación de incidentes regulados en los artículos 11, 19.1 y 19.2 del Real Decreto-ley 12/2018, de 7 de septiembre.

4. El CCN-CERT, en el caso previsto en el apartado anterior, y la Oficina de Coordinación de Ciberseguridad del Ministerio del Interior (OCC), en los supuestos previstos en el artículo 11.2 párrafo segundo del Real Decreto-ley 12/2018, de 7 de septiembre, requerirán al CSIRT de referencia, tras la primera notificación del incidente, al menos la siguiente información:

a) Confirmación de que son correctos los datos asignados al incidente, en particular verificando, si existe esta información, la validez de:

1.º La clasificación del incidente.
2.º La peligrosidad del incidente.
3.º El impacto del incidente.

b) Plan de acción del CSIRT para abordar la resolución técnica del incidente, si procede.

c) Cualquier información que permita determinar el posible impacto transfronterizo del incidente.

Siempre que sea posible se empleará la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes para las comunicaciones consideradas en este apartado.

Artículo 5. *Punto de contacto único.*

1. En su función de enlace para garantizar la cooperación transfronteriza de las autoridades competentes designadas conforme al artículo 9 del Real Decreto-ley 12/2018, de 7 de septiembre, con las autoridades competentes de otros Estados miembros de la Unión Europea, así como con el grupo de cooperación contemplado en el artículo 11 de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, y la red de CSIRT, el Consejo de Seguridad Nacional, a través del Departamento de Seguridad Nacional:

a) Comunicará a la Comisión Europea la lista de los operadores de servicios esenciales nacionales establecidos para cada sector y subsector a los que se refiere el artículo 6 del Real Decreto-ley 12/2018, de 7 de septiembre e informará a los puntos de contacto único de otros Estados sobre la intención de identificación de un operador de servicios esenciales de otro Estado miembro que ofrezca servicios en España.

b) Transmitirá a los puntos de contacto de otros Estados miembros de la Unión Europea afectados la información sobre incidentes con impacto transfronterizo que le transmitan las autoridades competentes o CSIRT de referencia, según lo establecido en el artículo 25 del Real Decreto-ley 12/2018, de 7 de septiembre.

c) Remitirá a los CSIRT de referencia y a las autoridades competentes nacionales la correspondiente información sobre incidentes que puedan tener efectos perturbadores en los servicios esenciales que reciba de los puntos de contacto de los correspondientes Estados miembros, para que adopten las medidas oportunas en el ejercicio de sus funciones respectivas.

d) Dictará las instrucciones pertinentes a las autoridades competentes para que elaboren, anualmente, el informe al que se refiere el artículo 27.1 del Real Decreto-ley 12/2018, de 7 de septiembre, sobre el tipo y número de incidentes comunicados, sus efectos en los servicios prestados o en otros servicios y su carácter nacional o transfronterizo dentro de la Unión Europea, teniendo en cuenta las indicaciones del grupo de cooperación respecto al formato y contenido de la información a transmitir.

e) Recabará de las autoridades competentes el informe anual al que se refiere la letra anterior, y elaborará un informe anual resumido sobre las notificaciones recibidas, que

remitirá al grupo de cooperación antes del 15 de febrero de cada año y, posteriormente, a las autoridades competentes y a los CSIRT de referencia, para su conocimiento.

2. Adicionalmente a las funciones de enlace previstas en el apartado anterior, y de conformidad con lo previsto en el artículo 9.2 del Real Decreto-ley 12/2018, de 7 de septiembre, el Consejo de Seguridad Nacional, a través de su comité especializado en materia de ciberseguridad, garantizará la coordinación de las actuaciones de las autoridades competentes mediante:

a) El fomento de la coherencia entre los requisitos de seguridad específicos que en su caso adopten las autoridades competentes, conforme a lo previsto en el artículo 6.6 de este real decreto.
b) El fomento de la coherencia entre las obligaciones específicas que en su caso establezcan las autoridades competentes, conforme a lo previsto en el artículo 8.3 de este real decreto.
c) El impulso de la coordinación de las disposiciones y actuaciones de las autoridades competentes y las actuaciones de los CSIRT de referencia con las disposiciones y actuaciones en materia de seguridad de la información de las autoridades de protección de datos y de seguridad pública.

3. Del mismo modo, el Consejo de Seguridad Nacional ejercerá las funciones de coordinación previstas en el apartado 2 anterior en los supuestos contemplados en el artículo 18 del Real Decreto-ley 12/2018, de 7 de septiembre.

CAPÍTULO III

Requisitos de seguridad

Artículo 6. *Medidas para el cumplimiento de las obligaciones de seguridad.*

1. Los operadores de servicios esenciales y los proveedores de servicios digitales deberán adoptar las medidas técnicas y de organización adecuadas y proporcionadas para gestionar los riesgos que afecten a la seguridad de las redes y sistemas de información utilizados para la prestación de sus servicios, tanto si se trata de redes y sistemas propios, como de proveedores externos.
2. En el caso de los operadores de servicios esenciales, deberán aprobar unas políticas de seguridad de las redes y sistemas de información, atendiendo a los principios de seguridad integral, gestión de riesgos, prevención, respuesta y recuperación, líneas de defensa, reevaluación periódica y segregación de tareas.
Dichas políticas considerarán, como mínimo, los siguientes aspectos:

a) Análisis y gestión de riesgos.
b) Gestión de riesgos de terceros o proveedores.
c) Catálogo de medidas de seguridad, organizativas, tecnológicas y físicas.
d) Gestión del personal y profesionalidad.
e) Adquisición de productos o servicios de seguridad.
f) Detección y gestión de incidentes.
g) Planes de recuperación y aseguramiento de la continuidad de las operaciones.
h) Mejora continua.
i) Interconexión de sistemas.
j) Registro de la actividad de los usuarios.

3. Las medidas de seguridad que se adopten por los operadores de servicios esenciales deberán tener en cuenta, en particular, la dependencia de las redes y sistemas de información y la continuidad de servicios o suministros contratados por el operador, así como las interacciones que presenten con redes y sistemas de información de terceros.
4. La relación de medidas adoptadas se formalizará en un documento denominado Declaración de Aplicabilidad de medidas de seguridad, que será suscrito por el responsable de seguridad de la información designado conforme a lo previsto en el artículo siguiente y que se incluirá en la política de seguridad que apruebe la Dirección de la organización. Dicho documento, que deberá remitirse a la autoridad competente respectiva en el plazo de seis

meses desde la designación del operador como operador de servicios esenciales, deberá revisarse, al menos, cada tres años. Tanto la Declaración de Aplicabilidad de medidas de seguridad inicial, como sus sucesivas revisiones serán objeto de supervisión por la autoridad competente respectiva, según se prevé en el artículo 14 de este real decreto.

5. Las medidas a las que se refieren los apartados anteriores tomarán como referencia las recogidas en el anexo II del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, en la medida en que sean aplicables, y se basarán, cuando sea posible, en otros esquemas nacionales de seguridad existentes.

Sin perjuicio de lo anterior, podrán tenerse en cuenta otros estándares reconocidos internacionalmente.

6. Las medidas adoptadas podrán ser complementadas con otras, atendiendo a necesidades específicas, entre ellas, la posibilidad de exigir un documento de aplicabilidad de los sistemas afectados por esta normativa, en aquellos operadores con entornos de sistemas de información especialmente complejos. En particular, se complementarán con las que, en su caso, establezcan con carácter específico las autoridades competentes, de conformidad con lo previsto en el artículo 16.4 y el artículo 32.2 del Real Decreto-ley 12/2018, de 7 de septiembre.

7. En la elaboración de las políticas de seguridad de las redes y sistemas de información se tendrán en cuenta los riesgos que se derivan del tratamiento de los datos personales, de acuerdo con el artículo 24 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante, Reglamento general de protección de datos). En caso de que el análisis de gestión de riesgos de acuerdo con el Reglamento general de protección de datos exija medidas adicionales a implantar respecto de las previstas en el Real Decreto 3/2010, de 8 de enero, se adoptarán las medidas de acuerdo con el artículo 24.1 del Reglamento general de protección de datos.

Artículo 7. *Responsable de la seguridad de la información.*

1. Los operadores de servicios esenciales designarán una persona, unidad u órgano colegiado, responsable de la seguridad de la información que ejercerá las funciones de punto de contacto y coordinación técnica con la autoridad competente y CSIRT de referencia que le corresponda de conformidad con lo previsto en el apartado tercero. En el supuesto de que el responsable de seguridad de la información sea una unidad u órgano colegiado, se deberá designar una persona física representante, así como un sustituto de este que asumirá sus funciones en casos de ausencia, vacante o enfermedad. El plazo para llevar a cabo dicha designación será de tres meses desde su designación como operador de servicios esenciales.

2. Los operadores de servicios esenciales comunicarán a la autoridad competente respectiva la designación del responsable de la seguridad de la información dentro del plazo establecido en el apartado anterior, así como los nombramientos y ceses que afecten a la designación del responsable de la seguridad de la información en el plazo de un mes desde que aquellos se produzcan.

3. El responsable de la seguridad de la información actuará como punto de contacto con la autoridad competente en materia de supervisión de los requisitos de seguridad de las redes y sistemas de información, y como punto de contacto especializado para la coordinación de la gestión de los incidentes con el CSIRT de referencia. Se desarrollarán bajo su responsabilidad, entre otras, las siguientes funciones:

a) Elaborar y proponer para aprobación por la organización, de conformidad con lo establecido en el artículo 6.2 de este real decreto, las políticas de seguridad, que incluirán las medidas técnicas y organizativas, adecuadas y proporcionadas, para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información utilizados y para prevenir y reducir al mínimo los efectos de los ciberincidentes que afecten a la organización y los servicios, de conformidad con lo dispuesto en el artículo 6.

b) Supervisar y desarrollar la aplicación de las políticas de seguridad, normativas y procedimientos derivados de la organización, supervisar su efectividad y llevar a cabo controles periódicos de seguridad.

c) Elaborar el documento de Declaración de Aplicabilidad de medidas de seguridad considerado en el artículo 6.3 párrafo segundo de este real decreto.

d) Actuar como capacitador de buenas prácticas en seguridad de las redes y sistemas de información, tanto en aspectos físicos como lógicos.

e) Remitir a la autoridad competente, a través del CSIRT de referencia y sin dilación indebida, las notificaciones de incidentes que tengan efectos perturbadores en la prestación de los servicios a los que se refiere el artículo 19.1 del Real Decreto-ley 12/2018, de 7 de septiembre.

f) Recibir, interpretar y supervisar la aplicación de las instrucciones y guías emanadas de la autoridad competente, tanto para la operativa habitual como para la subsanación de las deficiencias observadas.

g) Recopilar, preparar y suministrar información o documentación a la autoridad competente o el CSIRT de referencia, a su solicitud o por propia iniciativa.

El responsable de la seguridad de la información, para desarrollar estas funciones, se podrá apoyar en servicios prestados por terceros.

4. Los operadores de servicios esenciales garantizarán que el responsable de la seguridad de la información cumpla con los siguientes requisitos:

a) Contar con personal con conocimientos especializados y experiencia en materia de ciberseguridad, desde los puntos de vista organizativo, técnico y jurídico, adecuados al desempeño de las funciones indicadas en el apartado anterior.

b) Contar con los recursos necesarios para el desarrollo de dichas funciones.

c) Ostentar una posición en la organización que facilite el desarrollo de sus funciones, participando de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la seguridad, y manteniendo una comunicación real y efectiva con la alta dirección.

d) Mantener la debida independencia respecto de los responsables de las redes y los sistemas de información.

5. Siempre que concurran los requisitos de conocimiento, experiencia, independencia y, en su caso, titulación, las funciones y responsabilidades encomendadas al responsable de la seguridad de la información podrán compatibilizarse con las señaladas para el Responsable de Seguridad y Enlace y el Responsable de Seguridad del Esquema Nacional de Seguridad, de conformidad con lo dispuesto en la normativa aplicable a estas figuras.

CAPÍTULO IV

Gestión de incidentes de seguridad

Artículo 8. *Gestión de incidentes de seguridad.*

1. Los operadores de servicios esenciales y los proveedores de servicios digitales deberán gestionar y resolver los incidentes de seguridad que afecten a las redes y sistemas de información utilizados para la prestación de sus servicios. En el caso de redes y sistemas que no sean propios los operadores deberán tomar las medidas necesarias para garantizar que dichas acciones se lleven a cabo por los proveedores externos.

Esta obligación alcanza tanto a los incidentes detectados por el propio operador o proveedor como a los que les señalen el CSIRT de referencia o la autoridad competente, cuando tengan conocimiento de alguna circunstancia que haga sospechar de la existencia de un incidente.

2. Sin perjuicio de lo previsto en el artículo 28.1 del Real Decreto-ley 12/2018, de 7 de septiembre, los operadores de servicios esenciales y los proveedores de servicios digitales podrán solicitar voluntariamente ayuda especializada del CSIRT de referencia para la gestión de los incidentes, debiendo en tales casos atender a las indicaciones que reciban de este para resolver el incidente, mitigar sus efectos y reponer los sistemas afectados.

3. En la resolución de los incidentes, los operadores de servicios esenciales aplicarán los aspectos pertinentes de la política de gestión de la seguridad de las redes y sistemas de

información a la que se refiere el artículo 6, así como las obligaciones específicas que en su caso establezcan las autoridades competentes.

Artículo 9. *Obligaciones de notificación de incidentes de los operadores de servicios esenciales.*

1. Los operadores de servicios esenciales notificarán a la autoridad competente respectiva, a través del CSIRT de referencia, los incidentes que puedan tener efectos perturbadores significativos en dichos servicios, considerándose a tal efecto los incidentes con un nivel de impacto crítico, muy alto o alto, según el detalle que se especifica en el apartado 4 de la Instrucción nacional de notificación y gestión de ciberincidentes, que se contiene en el anexo de este real decreto.

Asimismo, notificarán los sucesos o incidencias que, por su nivel de peligrosidad, puedan afectar a las redes y sistemas de información empleados para la prestación de los servicios esenciales, aun cuando no hayan tenido todavía un efecto adverso real sobre aquellos. A estos efectos, se considerarán los incidentes con un nivel de peligrosidad crítico, muy alto o alto, según el detalle que se especifica en el apartado 3 de la citada Instrucción.

2. Sin perjuicio de lo anterior, las autoridades competentes podrán establecer, de conformidad con el artículo 19.5 del Real Decreto-ley 12/2018, de 7 de septiembre, obligaciones específicas de notificación que contemplen niveles diferentes a los previstos en la Instrucción nacional de notificación y gestión de ciberincidentes, así como factores y umbrales sectoriales específicos, aplicables a los operadores sometidos a su supervisión.

3. La notificación de un ciberincidente conforme a este real decreto no excluye ni sustituye la notificación que de los mismos hechos deba realizarse a otros organismos conforme a su normativa específica.

En particular, las obligaciones de notificación previstas en los apartados anteriores son independientes de las que deban realizarse a la Agencia Española de Protección de Datos conforme a lo previsto en el artículo 33 del Reglamento general de protección de datos, sin perjuicio de la cooperación entre autoridades prevista en el artículo 29 del Real Decreto-ley 12/2018, y la posibilidad de acceso por parte de la citada agencia a la plataforma común de notificación de incidentes prevista en su disposición adicional tercera.

A estos efectos, las notificaciones previstas en los apartados 1 y 2 de este artículo incluirán la información que, para los casos de violación de la seguridad de los datos personales, se contenga en los formularios aprobados por la Agencia Española de Protección de Datos.

Artículo 10. *Procedimientos de notificación de incidentes.*

1. Los CSIRT de referencia garantizarán un intercambio fluido de información con las autoridades competentes que correspondan, asegurando el adecuado seguimiento durante la gestión de los incidentes, así como el acceso a la información empleada en las distintas fases que componen la gestión de incidentes.

2. Los operadores de servicios esenciales realizarán las notificaciones a través del responsable de la seguridad de la información designado.

En el caso de que un operador de servicios esenciales reúna los criterios previstos en el artículo 6.2 del Real Decreto-ley 12/2018, de 7 de septiembre, sobre seguridad de las redes y sistemas de información, el responsable de la seguridad de la información se coordinará a estos efectos con el Responsable de Seguridad y Enlace previsto en el artículo 16 de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

3. Los operadores de servicios esenciales deberán realizar una primera notificación tan pronto como dispongan de información para determinar que se dan las circunstancias para la notificación, atendiendo a los factores y umbrales correspondientes.

Se efectuarán las notificaciones intermedias que sean precisas para actualizar o completar la información incorporada a la notificación inicial, e informar sobre la evolución del incidente, mientras este no esté resuelto, y se realizará una notificación final del incidente tras su resolución, informando del detalle de la evolución del suceso, la valoración de la probabilidad de su repetición, y las medidas correctoras que eventualmente tenga previsto

adoptar el operador. Los umbrales temporales exigidos para dichas notificaciones serán los recogidos en el anexo de este real decreto.

4. Las notificaciones incluirán, en cuanto esté disponible, la información que permita determinar cualquier efecto transfronterizo del incidente.

5. Lo establecido en los apartados anteriores será de aplicación a los proveedores de servicios digitales en tanto que no se regule de modo diferente en los actos de ejecución previstos en el artículo 16.9 de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

6. El CSIRT de referencia, en colaboración con la autoridad competente, valorará con prontitud dicha información con vistas a determinar si el incidente puede tener efectos perturbadores significativos para los servicios esenciales prestados en otros Estados miembros de la Unión Europea, informando en tal caso a través del punto de contacto único a los Estados miembros afectados.

Asimismo, la autoridad competente valorará, conjuntamente con el correspondiente CSIRT de referencia, la información sobre incidentes con posibles impactos transfronterizos que reciba de otros Estados miembros, y se lo indicará y transmitirá la información relevante a los operadores de servicios esenciales que puedan verse afectados.

Artículo 11. *Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes.*

1. El CCN-CERT en colaboración con el INCIBE-CERT y el ESPDEF-CERT del Mando Conjunto del Ciberespacio pondrá a disposición de todos los actores involucrados la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes a la que se refiere el artículo 19.4 del Real Decreto-ley 12/2018, de 7 de septiembre.

2. La plataforma permitirá el intercambio de información y el seguimiento de incidentes entre los operadores de servicios esenciales o proveedores de servicios digitales, las autoridades competentes y los CSIRT de referencia de manera segura y confiable, sin perjuicio de los requisitos específicos que apliquen en materia de protección de datos de carácter personal.

3. Esta plataforma deberá garantizar asimismo la disponibilidad, autenticidad, integridad y confidencialidad de la información, así como podrá emplearse también para dar cumplimiento a la exigencia de notificación derivada de regulaciones sectoriales, de acuerdo con el artículo 19.5 del Real Decreto-ley 12/2018, de 7 de septiembre.

4. La plataforma dispondrá asimismo de diversos canales de comunicación para su uso por parte de las autoridades competentes y los CSIRT de referencia. La plataforma garantizará el acceso de las autoridades competentes a toda la información relativa a la notificación y estado de situación de los incidentes de su ámbito de competencia que les permita efectuar en todo momento el necesario seguimiento y control de su estado de situación. Igualmente, las autoridades competentes tendrán acceso a través de la plataforma a datos estadísticos, en particular a los necesarios para generar los informes a los que hace mención el artículo 5.

5. Asimismo, la plataforma implementará el procedimiento de notificación y gestión de incidentes, que estará disponible durante todas las horas del día y todos los días del año, y dispondrá como mínimo de las siguientes capacidades:

a) Capacidad de gestión de ciberincidentes, con incorporación de taxonomía, criticidad y notificaciones a terceros, según lo establecido en el anexo.

b) Capacidad de intercambio de información sobre ciberamenazas.

c) Capacidad de análisis de muestras.

d) Capacidad de registro y notificación de vulnerabilidades.

e) Capacidad de comunicaciones seguras entre los actores involucrados en diferentes formatos y plataformas.

f) Capacidad de intercambio masivo de datos.

g) Generación de estadísticas e informes agregados.

Artículo 12. *Información sobre incidentes.*

1. Cuando las circunstancias lo permitan, los CSIRT de referencia proporcionarán a los operadores de servicios esenciales y a los proveedores de servicios digitales notificantes la información pertinente con respecto al seguimiento de la notificación de un incidente, en particular aquella que pueda facilitar la gestión eficaz del incidente.

2. Asimismo, las autoridades competentes y los CSIRT de referencia proporcionarán a los operadores de servicios esenciales y a los proveedores de servicios digitales que pudieran verse afectados por dichos incidentes la información que pudiera serles relevante para prevenir y en su caso resolver el incidente.

3. Al proporcionar la información a la que se refieren los apartados anteriores, las autoridades competentes y los CSIRT de referencia velarán por los intereses comerciales de los operadores de servicios esenciales y proveedores de servicios digitales, preservando la confidencialidad de la información que recaben de estos, de conformidad con lo establecido en el artículo 15 del Real Decreto-ley 12/2018, de 7 de septiembre.

Artículo 13. *Actuaciones ante incidentes con carácter presuntamente delictivo.*

En cumplimiento de lo dispuesto en el artículo 262 de la Ley de Enjuiciamiento Criminal, la OCC comunicará a la mayor brevedad posible al Ministerio Fiscal y, en su caso, a las Unidades orgánicas de Policía Judicial competentes, aquellos incidentes de seguridad que le sean notificados y que revistan carácter presuntamente delictivo, trasladando al tiempo la información que posea en relación con ello. A dicho fin podrá requerir de los operadores afectados o de los CSIRT de referencia cuanta información relacionada con el incidente se estime necesaria.

Artículo 14. *Consulta con otras autoridades.*

1. Las consultas con otras autoridades con competencia en materia de seguridad pública y seguridad ciudadana, previstas en el artículo 14.1 del Real Decreto-ley 12/2018, de 7 de septiembre, se realizarán a través de la OCC.

2. Las consultas relativas al resto de materias previstas en el citado artículo 14 se realizarán directamente a las autoridades competentes correspondientes.

CAPÍTULO V

Supervisión

Artículo 15. *Supervisión del cumplimiento de obligaciones de seguridad y de notificación de incidentes.*

1. Las autoridades competentes supervisarán en su ámbito de actuación el cumplimiento de las obligaciones de seguridad y de notificación de incidentes que sean de aplicación a los operadores de servicios esenciales y a los proveedores de servicios digitales de conformidad con el Real Decreto-ley 12/2018, de 7 de septiembre, y este real decreto.

2. Los operadores de servicios esenciales y los proveedores de servicios digitales colaborarán con la autoridad competente en dicha supervisión, facilitando las actuaciones de inspección, proporcionando toda la información que a tal efecto se les requiera, y aplicando las instrucciones dictadas, en su caso, para la subsanación de las deficiencias observadas.

3. El cumplimiento de las obligaciones de seguridad en las redes y sistemas de información podrá ser acreditado mediante la certificación en un esquema de seguridad que, previa consulta al CSIRT de referencia, sea reconocido por la autoridad competente.

4. Las autoridades competentes podrán realizar las actuaciones inspectoras que sean precisas para el ejercicio de su función de control. En particular, las actuaciones de inspección de las autoridades competentes, que podrán ser apoyadas por los CSIRT de referencia, tendrán por objeto:

a) Controlar el cumplimiento de las normas e instrucciones técnicas que, en su caso, resulten aplicables a los operadores sujetos a su supervisión.

b) Verificar el cumplimiento de las funciones del responsable de seguridad de la información designado por los operadores de servicios esenciales, según lo previsto en el artículo 7.3 de este real decreto.

c) Realizar las comprobaciones, inspecciones, pruebas y revisiones necesarias para verificar el cumplimiento de las medidas de seguridad previstas en el artículo 6, en particular, la política de seguridad de los operadores de servicios esenciales y la Declaración de aplicabilidad de medidas de seguridad.

De conformidad con lo previsto en el artículo 32.1 del Real Decreto-ley 12/2018, de 7 de septiembre, cuando el volumen o complejidad de las actuaciones de inspección que deban desarrollarse así lo aconseje, las autoridades competentes podrán requerir al operador de servicios esenciales la remisión de un informe de auditoría, elaborado por una entidad externa, solvente e independiente, sobre la seguridad de sus redes y sistemas de información.

5. Los CSIRT de referencia colaborarán con las autoridades competentes, cuando estas se lo requieran, en el ejercicio de las funciones a las que se refiere el apartado anterior. En particular, facilitarán asesoramiento técnico sobre la idoneidad de las medidas de seguridad adoptadas por los operadores de servicios esenciales y los proveedores de servicios digitales en virtud del artículo 6 de este real decreto.

Asimismo, cuando se trate de operadores con incidencia en la Defensa Nacional a que se refiere el artículo 4.2 de este real decreto, el ESPDEF-CERT del Mando Conjunto del Ciberespacio podrá colaborar en la supervisión con la autoridad competente.

6. En el caso de los proveedores de servicios digitales la supervisión se llevará a cabo de manera coordinada con las autoridades competentes correspondientes de los Estados miembros de la Unión Europea donde dichos proveedores presten servicios o tengan su establecimiento principal en la Unión.

Disposición adicional primera. *Designación del responsable de la seguridad de la información por los operadores de servicios esenciales designados.*

Los operadores de servicios esenciales designados conforme a lo previsto en la disposición adicional primera del Real Decreto-ley 12/2018, de 7 de septiembre, deberán comunicar a la autoridad competente respectiva la identidad del responsable de la seguridad de la información en el plazo de tres meses desde la entrada en vigor de este real decreto.

Disposición adicional segunda. *Orientaciones para la gestión de incidentes y cumplimiento de las obligaciones de notificación.*

El Consejo de Seguridad Nacional, a propuesta de su comité especializado en materia de ciberseguridad, y articuladas sus funciones como punto de contacto único a través del Departamento de Seguridad Nacional, podrá aprobar orientaciones en relación con la Instrucción Nacional de Notificación y Gestión de Incidentes recogida en el anexo, así como para la actualización de la Guía Nacional de Notificación y Gestión de Ciberincidentes, que incluyan directrices y recomendaciones para el cumplimiento de las obligaciones de notificación previstas en este real decreto, así como en el Real Decreto-ley 12/2018, de 7 de septiembre, con objeto de mejorar la coordinación y optimizar los recursos dedicados a la gestión de los incidentes que afecten a la seguridad de las redes y sistemas de información.

Disposición adicional tercera. *Régimen específico del Banco de España.*

Las disposiciones del presente real decreto se entenderán sin perjuicio de las competencias y funciones atribuidas al Banco de España, al Banco Central Europeo y al Sistema Europeo de Bancos Centrales, de conformidad con el Tratado de Funcionamiento de la Unión Europea, los Estatutos del Sistema Europeo de Bancos Centrales y del Banco Central Europeo, Reglamento (UE) n.º 1024/2013 del Consejo, de 15 de octubre de 2013, que encomienda al Banco Central Europeo tareas específicas respecto de políticas relacionadas con la supervisión prudencial de las entidades de crédito, y la Ley 13/1994, de 1 de junio, de Autonomía del Banco de España.

En lo no previsto en su normativa específica, y en cuanto sea compatible con su naturaleza, funciones e independencia, será de aplicación al Banco de España lo previsto en este real decreto.

Disposición adicional cuarta. *Supuesto de dependencia de proveedores externos.*

En referencia al artículo 19.3 del Real Decreto-ley 12/2018, de 7 de septiembre, cuando los operadores de servicios esenciales o proveedores de servicios digitales dependan de proveedores externos a los que les sea de aplicación la disposición adicional novena de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, el Equipo de Respuesta ante Emergencias Informáticas (CERT) competente del proveedor externo se corresponderá con:

a) El CCN-CERT, del Centro Criptológico Nacional, cuando el proveedor esté incluido en el ámbito subjetivo de aplicación de la Ley 40/2015, de 1 de octubre.

b) El INCIBE-CERT, del Instituto Nacional de Ciberseguridad de España, en el resto de los casos.

Disposición adicional quinta. *Tratamientos de datos de carácter personal.*

Los tratamientos de datos de carácter personal de las personas físicas se realizarán con estricta sujeción a lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a su libre circulación; en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y, en su caso, en la normativa sobre protección de datos personales especial o específica que resulte de aplicación.

Disposición adicional sexta. *Información sobre incidentes en el sistema financiero.*

Los CSIRT de referencia informarán al titular de la Secretaría de Estado de Economía y Apoyo a la Empresa, a través de la Secretaría General del Tesoro y Financiación Internacional, de los incidentes que puedan tener efectos perturbadores significativos en los servicios esenciales del sistema financiero. A estos efectos, se entenderá que tienen efectos perturbadores significativos cuando su umbral o nivel de impacto sea crítico, muy alto o alto, según lo señalado en el anexo de este real decreto.

Disposición transitoria única. *Desempeño transitorio de funciones en el sector energético.*

La Secretaría de Estado de Seguridad del Ministerio del Interior, a través de la Oficina de Coordinación de Ciberseguridad (OCC), desempeñará temporalmente las funciones atribuidas por este real decreto al departamento ministerial con competencias en materia de energía, hasta que este disponga de los recursos humanos necesarios con la formación adecuada para ejercer estas competencias de forma efectiva según lo previsto en el artículo 3 y, en todo caso, en un plazo máximo de 12 meses.

Disposición final primera. *Título competencial.*

Este real decreto se dicta al amparo de lo previsto en el artículo 149.1.21.ª y 29.ª de la Constitución, que atribuye al Estado competencia exclusiva en materia de régimen general de telecomunicaciones y seguridad pública, respectivamente.

Disposición final segunda. *Habilitación para el desarrollo normativo y aplicación.*

Se faculta a los titulares de los Ministerios de Asuntos Económicos y Transformación Digital, Interior y Defensa, así como a los titulares de los Ministerios y organismos relacionados en el artículo 3, para dictar conjunta o separadamente, según las materias de que se trate, y en el ámbito de sus respectivas competencias, las disposiciones que exijan el desarrollo y aplicación de este real decreto.

Disposición final tercera. *Entrada en vigor.*

El presente real decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

ANEXO

Instrucción nacional de notificación y gestión de ciberincidentes

1. Obligatoriedad de notificación

Los incidentes se asociarán a uno de los niveles de peligrosidad e impacto establecidos en esta instrucción, teniendo en cuenta la obligatoriedad de notificación de todos aquellos que se categoricen con un nivel CRÍTICO, MUY ALTO o ALTO para todos aquellos sujetos obligados a los que les sea aplicable esta «Instrucción nacional de notificación y gestión de ciberincidentes». En ese caso, los sujetos obligados deberán comunicar, en tiempo y forma, los incidentes que registren en sus redes y sistemas de información y que estén obligados a notificar por superar los umbrales de impacto o peligrosidad establecidos en esta instrucción.

Para la notificación de los incidentes de ciberseguridad se utilizará como criterio de referencia el nivel de peligrosidad que se asigne a un incidente, sin perjuicio de que a lo largo del desarrollo, mitigación o resolución del mismo, se categorice con un determinado nivel de impacto que haga aconsejable la comunicación del incidente a la autoridad competente o CSIRT de referencia.

En todo caso, cuando un determinado suceso pueda asociarse a más de un tipo de incidente debido a sus características potenciales, este se asociará a aquel que tenga un nivel de peligrosidad superior de acuerdo a los criterios expuestos en esta Instrucción.

2. Clasificación/taxonomía de los ciberincidentes

La siguiente Clasificación/Taxonomía de los ciberincidentes está alineada con la taxonomía aprobada por la Agencia de la Unión Europea para la Ciberseguridad (ENISA).

Esta Clasificación/Taxonomía de los ciberincidentes se empleará para la asignación de una clasificación específica a un incidente registrado en las redes y sistemas de información cuando se realice la comunicación a la autoridad competente o CSIRT de referencia.

Tabla 1. Clasificación/Taxonomía de los ciberincidentes

Clasificación	Tipo de incidente	Descripción y ejemplos prácticos
Contenido abusivo.	*Spam.*	Correo electrónico masivo no solicitado. El receptor del contenido no ha otorgado autorización válida para recibir un mensaje colectivo.
	Delitos de odio, contra la libertad o el honor.	Contenido difamatorio o discriminatorio. Ej.: ciberacoso, racismo, amenazas a una persona o dirigidas contra colectivos.
	Pornografía infantil, contenido sexual o violento inadecuado.	Material que represente de manera visual contenido relacionado con pornografía infantil, apología de la violencia, etc.
Contenido dañino.	Sistema infectado.	Sistema infectado con malware. Ej.: sistema, computadora o teléfono móvil infectado con un *rootkit*.
	Servidor C&C (Mando y Control).	Conexión con servidor de Mando y Control (C&C) mediante malware o sistemas infectados.
	Distribución de malware.	Recurso usado para distribución de malware. Ej.: recurso de una organización empleado para distribuir malware.
	Configuración de malware.	Recurso que aloje ficheros de configuración de malware Ej.: ataque de *webinjects* para troyano.
Obtención de información.	Escaneo de redes (*scanning*).	Envío de peticiones a un sistema para descubrir posibles debilidades. Se incluyen también procesos de comprobación o testeo para recopilar información de alojamientos, servicios y cuentas. Ej.: peticiones DNS, ICMP, SMTP, escaneo de puertos.
	Análisis de paquetes (*sniffing*).	Observación y grabación del tráfico de redes.
	Ingeniería social.	Recopilación de información personal sin el uso de la tecnología. Ej.: mentiras, trucos, sobornos, amenazas.
Intento de intrusión.	Explotación de vulnerabilidades conocidas.	Intento de compromiso de un sistema o de interrupción de un servicio mediante la explotación de vulnerabilidades con un identificador estandarizado (véase CVE). Ej.: desbordamiento de *buffer*, puertas traseras, *cross site scripting* (XSS).
	Intento de acceso con vulneración de credenciales.	Múltiples intentos de vulnerar credenciales. Ej.: intentos de ruptura de contraseñas, ataque por fuerza bruta.
	Ataque desconocido.	Ataque empleando *exploit* desconocido.
Intrusión.	Compromiso de cuenta con privilegios.	Compromiso de un sistema en el que el atacante ha adquirido privilegios.
	Compromiso de cuenta sin privilegios.	Compromiso de un sistema empleando cuentas sin privilegios.
	Compromiso de aplicaciones.	Compromiso de una aplicación mediante la explotación de vulnerabilidades de software. Ej.: inyección SQL.
	Robo.	Intrusión física. Ej.: acceso no autorizado a Centro de Proceso de Datos.

Clasificación	Tipo de incidente	Descripción y ejemplos prácticos
Disponibilidad.	DoS (Denegación de servicio).	Ataque de denegación de servicio. Ej.: envío de peticiones a una aplicación *web* que provoca la interrupción o ralentización en la prestación del servicio.
	DDoS (Denegación distribuida de servicio).	Ataque de denegación distribuida de servicio. Ej.: inundación de paquetes SYN, ataques de reflexión y amplificación utilizando servicios basados en UDP.
	Mala configuración.	Configuración incorrecta del software que provoca problemas de disponibilidad en el servicio. Ej.: Servidor DNS con el KSK de la zona raíz de DNSSEC obsoleto.
	Sabotaje.	Sabotaje físico. Ej.: cortes de cableados de equipos o incendios provocados.
	Interrupciones.	Interrupciones por causas ajenas. Ej.: desastre natural.
Compromiso de la información.	Acceso no autorizado a información.	Acceso no autorizado a información. Ej.: robo de credenciales de acceso mediante interceptación de tráfico o mediante el acceso a documentos físicos.
	Modificación no autorizada de información.	Modificación no autorizada de información. Ej.: modificación por un atacante empleando credenciales sustraídas de un sistema o aplicación o encriptado de datos mediante *ransomware*.
	Pérdida de datos.	Pérdida de información Ej.: pérdida por fallo de disco duro o robo físico.
Fraude.	Uso no autorizado de recursos.	Uso de recursos para propósitos inadecuados, incluyendo acciones con ánimo de lucro. Ej.: uso de correo electrónico para participar en estafas piramidales.
	Derechos de autor.	Ofrecimiento o instalación de software carente de licencia u otro material protegido por derechos de autor. Ej.: Warez.
	Suplantación.	Tipo de ataque en el que una entidad suplanta a otra para obtener beneficios ilegítimos.
	Phishing.	Suplantación de otra entidad con la finalidad de convencer al usuario para que revele sus credenciales privadas.
Vulnerabilidad.	Criptografía débil.	Servicios accesibles públicamente que puedan presentar criptografía débil. Ej.: servidores web susceptibles de ataques POODLE/FREAK.
	Amplificador DDoS.	Servicios accesibles públicamente que puedan ser empleados para la reflexión o amplificación de ataques DDoS. Ej.: DNS *open-resolvers* o Servidores NTP con monitorización *monlist*.
	Servicios con acceso potencial no deseado.	Ej.: Telnet, RDP o VNC.
	Revelación de información.	Acceso público a servicios en los que potencialmente pueda relevarse información sensible. Ej.: SNMP o Redis.
	Sistema vulnerable.	Sistema vulnerable. Ej.: mala configuración de *proxy* en cliente (WPAD), versiones desfasadas de sistema.
Otros.	Otros.	Todo aquel incidente que no tenga cabida en ninguna categoría anterior.
	APT.	Ataques dirigidos contra organizaciones concretas, sustentados en mecanismos muy sofisticados de ocultación, anonimato y persistencia. Esta amenaza habitualmente emplea técnicas de ingeniería social para conseguir sus objetivos junto con el uso de procedimientos de ataque conocidos o genuinos.

3. Nivel de peligrosidad del ciberincidente

El indicador de peligrosidad determina la potencial amenaza que supondría la materialización de un incidente en los sistemas de información o comunicación del ente afectado, así como para los servicios prestados o la continuidad de negocio en caso de haberla. Este indicador se fundamenta en las características intrínsecas a la tipología de amenaza y su comportamiento.

Los incidentes se asociarán a alguno de los siguientes niveles de peligrosidad: CRÍTICO, MUY ALTO, ALTO, MEDIO, BAJO.

Nivel crítico:

– APT.

Nivel muy alto:

– Distribución de malware.
– Configuración de malware.
– Robo.
– Sabotaje.
– Interrupciones.

Nivel alto:

– Pornografía infantil, contenido sexual o violento inadecuado.
– Sistema infectado.
– Servidor C&C (Mando y Control).
– Compromiso de aplicaciones.
– Compromiso de cuentas con privilegios.
– Ataque desconocido.
– DoS (Denegación de servicio).
– DDoS (Denegación distribuida de servicio).
– Acceso no autorizado a información.
– Modificación no autorizada de información.
– Pérdida de datos.
– *Phishing.*

Nivel medio:

– Discurso de odio.
– Ingeniería social.
– Explotación de vulnerabilidades conocidas.
– Intento de acceso con vulneración de credenciales.
– Compromiso de cuentas sin privilegios.
– Desconfiguración.
– Uso no autorizado de recursos.
– Derechos de autor.
– Suplantación.
– Criptografía débil.
– Amplificador DDoS.
– Servicios con acceso potencial no deseado.
– Revelación de información.
– Sistema vulnerable.

Nivel bajo:

– *Spam.*
– Escaneo de redes (*scanning*).
– Análisis de paquetes (*sniffing*).
– Otros.

4. Nivel de impacto del ciberincidente

El indicador de impacto de un ciberincidente se determinará evaluando las consecuencias que tal ciberincidente ha tenido en las funciones y actividades de la organización afectada, en sus activos o en los individuos afectados. De acuerdo a ello, se tienen en cuenta aspectos como las consecuencias potenciales o materializadas que provoca una determinada amenaza en un sistema de información y/o comunicación, así como en la propia entidad afectada (organismos públicos o privados, y particulares).

Los criterios empleados para la determinación del nivel de impacto asociado a un ciberincidente atienden a los siguientes parámetros:

– Impacto en la Seguridad Nacional o en la seguridad ciudadana.
– Efectos en la prestación de un servicio esencial o en una infraestructura crítica.
– Tipología de la información o sistemas afectados.
– Grado de afectación a las instalaciones de la organización.
– Posible interrupción en la prestación del servicio normal de la organización.
– Tiempo y costes propios y ajenos hasta la recuperación del normal funcionamiento de las instalaciones.
– Pérdidas económicas.
– Extensión geográfica afectada.
– Daños reputacionales asociados.

Los incidentes se asociarán a alguno de los siguientes niveles de impacto: CRÍTICO, MUY ALTO, ALTO, MEDIO, BAJO, SIN IMPACTO.

Nivel crítico:

– Afecta apreciablemente a la Seguridad Nacional.
– Afecta a la seguridad ciudadana, con potencial peligro para la vida de las personas.
– Afecta a una infraestructura crítica.
– Afecta a sistemas clasificados SECRETO.
– Afecta a más del 90 % de los sistemas de la organización.
– Interrupción en la prestación del servicio superior a 24 horas y superior al 50 % de los usuarios.
– El ciberincidente precisa para resolverse más de 100 Jornadas-Persona.
– Impacto económico superior al 0,1 % del Producto Interior Bruto (PIB) actual.
– Extensión geográfica supranacional.
– Daños reputacionales muy elevados y cobertura continua en medios de comunicación internacionales.

Nivel muy alto:

– Afecta a la seguridad ciudadana con potencial peligro para bienes materiales.
– Afecta apreciablemente a actividades oficiales o misiones en el extranjero.
– Afecta a un servicio esencial.
– Afecta a sistemas clasificados RESERVADO.
– Afecta a más del 75 % de los sistemas de la organización.
– Interrupción en la prestación del servicio superior a 8 horas y superior al 35 % de los usuarios.
– El ciberincidente precisa para resolverse entre 30 y 100 Jornadas-Persona.
– Impacto económico entre el 0,07 % y el 0,1 % del PIB actual.
– Extensión geográfica superior a 4 Comunidades Autónomas (CC.AA.) o un territorio de Interés Singular (TIS, se considera como tal a las ciudades de Ceuta y Melilla y a cada una de las islas que forman los archipiélagos de las islas Baleares y las islas Canarias).
– Daños reputacionales a la imagen del país (marca España).
– Daños reputacionales elevados y cobertura continua en medios de comunicación nacionales.

Nivel alto:

– Afecta a más del 50 % de los sistemas de la organización.
– Interrupción en la prestación del servicio superior a 1 hora y superior al 10 % de usuarios.
– El ciberincidente precisa para resolverse entre 5 y 30 Jornadas-Persona.
– Impacto económico entre el 0,03 % y el 0,07 % del PIB actual.
– Extensión geográfica superior a 3 CC.AA.
– Daños reputacionales de difícil reparación, con eco mediático (amplia cobertura en los medios de comunicación) y afectando a la reputación de terceros.

Nivel medio:

– Afecta a más del 20 % de los sistemas de la organización.
– Interrupción en la presentación del servicio superior al 5 % de usuarios.
– El ciberincidente precisa para resolverse entre 1 y 5 Jornadas-Persona.
– Impacto económico entre el 0,001 % y el 0,03 % del PIB actual.
– Extensión geográfica superior a 2 CC.AA.
– Daños reputacionales apreciables, con eco mediático (amplia cobertura en los medios de comunicación).

Nivel bajo:

– Afecta a los sistemas de la organización.
– Interrupción de la prestación de un servicio.
– El ciberincidente precisa para resolverse menos de 1 Jornada-Persona.
– Impacto económico entre el 0,0001 % y el 0,001 % del PIB actual.
– Extensión geográfica superior a 1 CC.AA.
– Daños reputacionales puntuales, sin eco mediático.

Sin impacto:

– No hay ningún impacto apreciable.

5. Información a notificar a la autoridad competente en caso de incidente

El sujeto obligado comunicará, en la notificación inicial, todos aquellos campos acerca de los que tenga conocimiento en ese momento de acuerdo a la siguiente tabla, siendo posteriormente preceptiva la cumplimentación de todos los campos de la tabla en la notificación final del incidente.

Tabla 2. Información a notificar a la autoridad competente en caso de incidente

Qué notificar	Descripción
Asunto.	Frase que describa de forma general el incidente. Este campo lo heredarán todas las notificaciones asociadas al incidente.
OSE/PSD.	Denominación del operador de servicios esenciales o proveedor de servicios digitales que notifica.
Sector estratégico.	Energía, transporte, financiero, etc.
Fecha y hora del incidente.	Indicar con la mayor precisión posible cuándo ha ocurrido el ciberincidente.
Fecha y hora de detección del incidente.	Indicar con la mayor precisión posible cuándo se ha detectado el ciberincidente.
Descripción.	Describir con detalle lo sucedido.
Recursos tecnológicos afectados.	Indicar la información técnica sobre el número y tipo de activos afectados por el ciberincidente, incluyendo direcciones IP, sistemas operativos, aplicaciones, versiones….
Origen del incidente.	Indicar la causa del incidente si se conoce. Apertura de un fichero sospechoso, conexión de un dispositivo USB, acceso a una página web maliciosa, etc.
Taxonomía (clasificación).	Posible clasificación y tipo de ciberincidente en función de la taxonomía descrita.
Nivel de peligrosidad.	Especificar el nivel de peligrosidad asignado a la amenaza.
Nivel de impacto.	Especificar el nivel de impacto asignado al incidente.
Impacto transfronterizo.	Indicar si el incidente tiene impacto transfronterizo en algún Estado miembro de la Unión Europea.
Plan de acción y contramedidas.	Actuaciones realizadas hasta el momento en relación al ciberincidente. Indicar el Plan de acción seguido junto con las contramedidas implantadas.
Afectación.	Indicar si el afectado es una empresa o un particular, y las afectaciones según el nivel de impacto asignado.
Medios necesarios para la resolución (J-P).	Capacidad empleada en la resolución del incidente en Jornadas-Persona.
Impacto económico estimado (Si se conoce).	Costes asociados al incidente, tanto de carácter directo como indirecto.
Extensión geográfica (Si se conoce).	Local, autonómico, nacional, supranacional, etc.
Daños reputacionales (Si se conocen).	Afectación a la imagen corporativa del operador.
Adjuntos.	Indicar la relación de documentos adjuntos que se aportan para ayudar a conocer la causa del problema o a su resolución (capturas de pantalla, ficheros de registro de información, correos electrónicos, etc.).
Regulación afectada.	ENS / RGPD / NIS / PIC / Otros.
Se requiere actuación de FFCCSE.	Si / No.

6. Ventana temporal de reporte

Todos aquellos sujetos obligados que se vean afectados por un incidente de obligada notificación a la autoridad competente, a través del CSIRT de referencia, remitirán, en tiempo y forma, aquellas notificaciones inicial, intermedia y final requeridas de acuerdo a la siguiente ventana temporal de reporte.

– La notificación inicial es una comunicación consistente en poner en conocimiento y alertar de la existencia de un incidente.
– La notificación intermedia es una comunicación mediante la que se actualizarán los datos disponibles en ese momento relativos al incidente comunicado.
– La notificación final es una comunicación final mediante la que se amplían y confirman los datos definitivos relativos al incidente comunicado.

No obstante lo anterior, se aportarán todas aquellas notificaciones adicionales intermedias o posteriores que se consideren necesarias.

Tabla 3. Ventana temporal de reporte

Nivel de peligrosidad o impacto	Notificación inicial	Notificación intermedia	Notificación final
CRÍTICO.	Inmediata.	24/48 horas.	20 días.
MUY ALTO.	Inmediata.	72 horas.	40 días.
ALTO.	Inmediata.	–	–
MEDIO.	–	–	–
BAJO.	–	–	–

Los tiempos reflejados en la tabla 3 para la «notificación intermedia» y la «notificación final» tienen como referencia el momento de remisión de la «notificación inicial». La «notificación inicial» tiene como referencia de tiempo el momento de tener conocimiento del incidente.

7. Definiciones y conceptos

La descripción de las conductas aquí incluidas tiene carácter técnico y se entiende a los meros efectos de la notificación y gestión de ciberincidentes. Como tal, es independiente tanto de la calificación de los hechos, como de la aplicación por parte de la autoridad judicial

de los tipos penales establecidos en la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

Contenido abusivo:

– Correo masivo no solicitado (*spam*): correo electrónico no solicitado que se envía a un gran número de usuarios, o bien una alta tasa de correos electrónicos enviados a un mismo usuario en un corto espacio de tiempo.

– Acoso: referido a acoso virtual o ciberacoso, se trata del uso de medios de comunicación digitales para acosar a una persona, o grupo de personas, mediante ataques personales, divulgación de información privada o íntima, o falsa.

– Extorsión: obligar a una persona o mercantil, mediante el empleo de violencia o intimidación, a realizar u omitir actos con la intención de producir un perjuicio a esta, o bien con ánimo de lucro de la que lo provoca.

– Mensajes ofensivos: comunicaciones no esperadas o deseadas, así como acciones o expresiones que lesionan la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación.

– Delito: cualquier acción tipificada como delito de acuerdo a lo establecido en la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

– Pederastia: cualquier comportamiento relacionado con los descritos en el título VIII la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, relativos a la captación o utilización de menores de edad o personas con discapacidad necesitadas de especial protección en actos que atenten contra su indemnidad o libertad sexual.

– Racismo: cualquier infracción penal, incluyendo infracciones contra las personas o las propiedades, donde la víctima, el local o el objetivo de la infracción se elija por su real o percibida, conexión, simpatía, filiación, apoyo o pertenencia a un grupo social, raza, religión o condición sexual.

– Apología de la violencia: exposición, ante una concurrencia de personas o por cualquier medio de difusión, de ideas o doctrinas que ensalcen el crimen o enaltezcan a su autor.

Contenido dañino:

– *Malware* (código dañino): palabra que deriva de los términos *malicious* y *software*. Cualquier pieza de *software* que lleve a cabo acciones como extracción de datos u otro tipo de alteración de un sistema puede categorizarse como *malware*. Así pues *malware* es un término que engloba varios tipos de programas dañinos.

– Virus: tipo de *malware* cuyo principal objetivo es modificar o alterar el comportamiento de un sistema informático sin el permiso o consentimiento del usuario. Se propaga mediante la ejecución en el sistema de software, archivos o documentos con carga dañina, adquiriendo la capacidad de replicarse de un sistema a otro. Los métodos más comunes de infección se dan a través de dispositivos extraíbles, descargas de Internet y archivos adjuntos en correos electrónicos. No obstante también puede hacerlo a través de *scripts*, documentos, y vulnerabilidades XSS presentes en la *web*. Es reseñable que un virus requiere la acción humana para su propagación a diferencia de otro *malware*, véase Gusano.

– Gusano: programa malicioso que tiene como característica principal su alto grado de dispersabilidad. Su fin es replicarse a nuevos sistemas para infectarlos y seguir replicándose a otros equipos informáticos, aprovechándose de todo tipo de medios como el correo electrónico, IRC, FTP, correo electrónico, P2P y otros protocolos específicos o ampliamente utilizados.

– Troyano: tipo de *malware* que se enmascara como *software* legítimo con la finalidad de convencer a la víctima para que instale la pieza en su sistema. Una vez instalado, el *software* dañino tiene la capacidad de desarrollar actividad perjudicial en segundo plano. Un troyano no depende una acción humana y no tiene la capacidad de replicarse, no obstante puede tener gran capacidad dañina en un sistema a modo de troyanos o explotando vulnerabilidades de *software*.

– Programa espía (*spyware*): tipo de *malware* que espía las actividades de un usuario sin su conocimiento o consentimiento. Estas actividades pueden incluir *keyloggers*,

monitorizaciones, recolección de datos así como robo de datos. Los *spyware* se pueden difundir como un troyano o mediante explotación de *software*.

– *Rootkit*: conjunto de *software* dañino que permite el acceso privilegiado a áreas de una máquina, mientras que al mismo tiempo se oculta su presencia mediante la corrupción del Sistema Operativo u otras aplicaciones. Denotar que por maquina se entiende todo el espectro de sistemas IT, desde *smartphones* hasta ICS. El propósito por tanto de un *rootkit* es enmascarar eficazmente *payloads* y permitir su existencia en el sistema.

– *Dialer*: tipología de *malware* que se instala en una máquina y, de forma automática y sin consentimiento del usuario, realiza marcaciones telefónicas a número de tarificación especial. Estas acciones conllevan costes económicos en la víctima al repercutir el importe de la comunicación.

– *Ransomware*: se engloba bajo este epígrafe a aquel *malware* que infecta una máquina, de modo que el usuario es incapaz de acceder a los datos almacenados en el sistema. Normalmente la víctima recibe posteriormente algún tipo de comunicación en la que se le coacciona para que se pague una recompensa que permita acceder al sistema y los archivos bloqueados.

– *Bot* dañino: una *botnet* es el nombre que se emplea para designar a un conjunto de máquinas controladas remotamente con finalidad generalmente maliciosa. Un *bot* es una pieza de *software* maliciosa que recibe órdenes de un atacante principal que controla remotamente la máquina. Los servidores C&C habilitan al atacante para controlar los *bots* y que ejecuten las órdenes dictadas remotamente.

– RAT: del inglés *Remote Access Tool*, se trata de una funcionalidad específica de control remoto de un sistema de información, que incorporan determinadas familias o muestras de *software* dañino (*malware*).

– C&C: del inglés *Command and Control*, se refiere a paneles de mando y control (también referenciados como C2), por el cual atacantes cibernéticos controlan determinados equipos *zombie* infectados con muestras de la misma familia de *software* dañino. El panel de comando y control actúa como punto de referencia, control y gestión de los equipos infectados.

– Conexión sospechosa: todo intercambio de información a nivel de red local o pública, cuyo origen o destino no esté plenamente identificado, así como la legitimidad de los mismos.

Obtención de información:

– Escaneo de puertos (*Scanning*): análisis local o remoto mediante *software*, del estado de los puertos de una máquina conectada a una red. La finalidad de esta acción es la de obtener información relativa a la identificación de los servicios activos y las posibles vulnerabilidades que puedan existir en la red.

– Escaneo de red (*Scanning*): análisis local o remoto mediante *software*, del estado de una red. La finalidad de esta acción es la de obtener información relativa a la identificación de los servicios activos y las posibles vulnerabilidades que puedan existir en la red.

– Escaneo de tecnologías: análisis local o remoto mediante *software*, de las tecnologías presentes o disponibles en una red determinada o un sistema de información concreto, mediante el cual se obtienen las referencias del *hardware/software* presente, así como su versión, y potenciales vulnerabilidades.

– Transferencia de zona DNS (AXFR IXFR): transacción de los servidores DNS utilizada para la replicación de las bases de datos entre un servidor primario y los secundarios. Estas transacciones pueden ser completas (AXFR) o incrementales (IXFR).

– Análisis de paquetes (*Sniffing*): análisis mediante *software* del tráfico de una red con la finalidad de capturar información. El tráfico que viaje no cifrado podrá ser capturado y leído por un atacante.

– Ingeniería social: técnicas que buscan la revelación de información sensible de un objetivo, generalmente mediante el uso de métodos persuasivos y con ausencia de voluntad o conocimiento de la víctima.

– *Phishing*: estafa cometida a través de medios telemáticos mediante la cual el estafador intenta conseguir, de usuarios legítimos, información confidencial (contraseñas, datos bancarios, etc.) de forma fraudulenta empleando métodos de ingeniería social.

– *Spear Phishing*: variante del *phishing* mediante la que el atacante focaliza su actuación sobre un objetivo concreto.

Intrusiones:

– Explotación: cualquier práctica mediante la cual un atacante cibernético vulnera un sistema de información y/o comunicación, con fines ilícitos o para los cuales no está debidamente autorizado.

– Inyección SQL: tipo de explotación, consistente en la introducción de cadenas mal formadas de SQL, o cadenas que el receptor no espera o controla debidamente; las cuales provocan resultados no esperados en la aplicación o programa objetivo, y por la cual el atacante produce efectos inesperados y para los que no está autorizado en el sistema objetivo.

– *Cross Site Scripting* XSS (Directo o Indirecto): ataque que trata de explotar una vulnerabilidad presente en aplicaciones web, por la cual un atacante inyecta sentencias mal formadas o cadenas que el receptor no espera o controla debidamente.

– *Cross Site Request Forgery* (CSFR): falsificación de petición en sitios cruzados. Es un tipo de *exploit* dañino de un sitio *web* en el que comandos no autorizados son transmitidos por un usuario en el cual el sitio web confía. Esta vulnerabilidad es conocida también por otros nombres como XSRF, enlace hostil, ataque de un clic, cabalgamiento de sesión, y ataque automático. Al contrario que en los ataques XSS, los cuales explotan la confianza que un usuario tiene en un sitio en particular, el *Cross Site Request Forgery* explota la confianza que un sitio tiene en un usuario en particular.

– *Defacement*: tipología de ataque a sitios web en el que se implementa un cambio en la apariencia visual de la página. Para ello suelen emplearse técnicas como inyecciones SQL o algún tipo de vulnerabilidad existente en la página o en el servidor.

– Inclusión de ficheros (RFI y LFI): vulnerabilidad que permite a un atacante mostrar o ejecutar archivos remotos alojados en otros servidores a causa de una mala programación de la página que contiene funciones de inclusión de archivos. La inclusión local de archivos (LFI) es similar a la vulnerabilidad de Inclusión de archivos remotos, excepto que en lugar de incluir archivos remotos solo se pueden incluir archivos locales, es decir, archivos en el servidor actual para su ejecución.

– Evasión de sistemas de control: proceso por el cual una muestra de software dañino, o un conjunto de acciones orquestadas por un atacante cibernético, consiguen vulnerar o esquivar los sistemas o políticas de seguridad establecidas por un determinado sistema de información y comunicación.

– *Pharming*: ataque informático que aprovecha vulnerabilidades de los servidores DNS (*Domain Name System*). Al tratar de acceder el usuario al sitio *web*, el navegador redirigirá automáticamente al usuario a una dirección IP donde se aloja una *web* maliciosa que suplanta la auténtica, y en la que el atacante podrá obtener información sensible de los usuarios.

– Ataque por fuerza bruta: proceso por el cual un atacante trata de vulnerar un sistema de validación por credenciales de acceso, contraseña o similar, mediante el empleo de todas las combinaciones posibles, con el fin de acceder a sistemas de información y/o comunicación para los cuales no tiene privilegios o autorización.

– Ataque por diccionario: proceso por el cual un atacante trata de vulnerar un sistema de validación por credenciales de acceso, contraseña o similar, mediante el empleo de un diccionario previamente generado con determinadas combinaciones de caracteres, con el fin de acceder a sistemas de información y/o comunicación para los cuales no tiene privilegios o autorización.

– Robo de credenciales de acceso: acceso o sustracción no autorizada a credenciales de acceso a sistemas de información y/o comunicación.

Disponibilidad:

– DoS (*Denial of Service*) o ataque de denegación de servicio: conjunto de técnicas que tienen por objetivo dejar un servidor inoperativo. Mediante este tipo de ataques se busca sobrecargar un servidor y de esta forma impedir que los usuarios legítimos puedan utilizar

los servicios por prestados por él. El ataque consiste en saturar con peticiones de servicio al servidor, hasta que este no puede atenderlas, provocando su colapso.

– DDoS (*Distributed Denial of Service*) o denegación distribuida de servicio: variante de DoS en el que la remisión de peticiones se lleva a cabo de forma coordinada desde varios puntos hacia un mismo destino. Para ello se emplean redes de *bots*, generalmente sin el conocimiento de los usuarios.

– Mala configuración: fallo de configuración en el *software* que está directamente asociado con una pérdida de disponibilidad de un servicio.

– Sabotaje/Terrorismo/Vandalismo: ataques implementados con el objetivo de provocar la interrupción o degradación de la prestación de un servicio, provocando daños relevantes en la continuidad del servicio de una institución o daños reputacionales relevantes cometidos con propósitos ideológicos, políticos o religiosos.

– Disrupción sin intención dañina: acciones que pueden provocar la interrupción o degradación de la prestación de un servicio, provocando daños relevantes en la continuidad del servicio de una institución o daños reputaciones relevantes.

– Inundación SYN o UDP: procedimientos usados para la realización de ataque DoS o DDoS consistente en iniciar una gran cantidad de sesiones impidiendo al servidor atender las peticiones licitas.

– DNS *Open-Resolver*: servidor DNS capaz resolver consultas DNS recursivas procedentes de cualquier origen de Internet. Este tipo de servidores suele emplearse por usuarios malintencionados para la realización de ataques DDoS.

Compromiso de la información:

– Acceso no autorizado a la información o ciberespionaje: proceso por el cual un usuario no autorizado accede a consultar contenido para el cual no está autorizado.

– Modificación no autorizada de información: proceso por el cual un usuario no autorizado accede a modificar contenido para el cual no está autorizado.

– Borrado no autorizado de información: proceso por el cual un usuario no autorizado accede a borrar contenido para el cual no está autorizado.

– Exfiltración de información: proceso por el cual un usuario difunde información en canales o fuentes en las cuales no está prevista o autorizada la compartición de esa información.

– Acceso no autorizado a sistemas: proceso por el cual un usuario accede sin vulnerar ningún servicio, sistema o red, a sistemas de información y/o comunicación para los cuales no está debidamente autorizado, o no tiene autorización tácita o manifiesta.

– Ataque POODLE / Ataque FREAK: proceso por el que se consigue que un servidor haga uso de un protocolo de comunicaciones no seguro, que originalmente no estaba previsto, con el objetivo de poder exfiltrar información.

Fraude:

– Uso no autorizado de recursos: empleo de tecnologías y/o servicios por usuarios que no están debidamente autorizados por la Dirección o negociado competente.

– Suplantación de identidad: actividad maliciosa en la que un atacante se hace pasar por otra persona para cometer algún tipo de fraude o acoso.

– Derechos de propiedad intelectual: la propiedad intelectual es el conjunto de derechos que corresponden a los autores y a otros titulares (artistas, productores, organismos de radiodifusión…) respecto de las obras y prestaciones fruto de su creación.

– Otros fraudes: engaño económico con la intención de conseguir un beneficio, y con el cual alguien resulta perjudicado.

Vulnerabilidades:

– Tecnología vulnerable: conocimiento por parte de los administradores de tecnologías, servicios o redes, de vulnerabilidades presentes en estas.

– Política de seguridad precaria: política de seguridad de la organización deficiente, mediante la cual existe la posibilidad de que durante un espacio de tiempo determinado, atacantes cibernéticos realizaron accesos no autorizados a sistemas de información, no pudiendo determinar fehacientemente este extremo.

Otros:

– Ciberterrorismo: delitos informáticos previstos en los artículo 197 bis y ter y 264 a 264 quater de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal cuando dichos delitos se cometan con las finalidades previstas en el artículo 573.1 del mismo texto. Estas finalidades son:

• Subvertir el orden constitucional, o suprimir o desestabilizar gravemente el funcionamiento de las instituciones políticas o de las estructuras económicas o sociales del Estado, u obligar a los poderes públicos a realizar un acto o a abstenerse de hacerlo.
• Alterar gravemente la paz pública.
• Desestabilizar gravemente el funcionamiento de una organización internacional.
• Provocar un estado de terror en la población o en una parte de ella.

– Daños informáticos PIC: delitos informáticos previstos en los artículos 264.2 3.º y 4.º de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, relacionadas con el borrado, dañado, alteración, supresión, o inaccesibilidad de datos, programas informáticos o documentos electrónicos de una Infraestructura Crítica. Así como conductas graves relacionadas con los términos anteriores que afecten a la prestación de un servicio esencial.

– APT (*Advanced Persistent Threat* o Amenaza Persistente Avanzada)/AVT (*Advanced Volatility Threat*): ataques dirigidos contra organizaciones concretas, sustentados en mecanismos muy sofisticados de ocultación, anonimato y persistencia. Esta amenaza habitualmente emplea técnicas de ingeniería social para conseguir sus objetivos junto con el uso de procedimientos de ataque conocidos o genuinos.

– Dominios DGA: procedimiento para generar de forma dinámica dominios donde se alojarán los servidores de Comando y Control, técnica usada en redes *Botnet* para dificultar su detención.

– Criptografía: técnica que consiste en cifrar un mensaje, conocido como texto en claro, convirtiéndolo en un mensaje cifrado o criptograma, que resulta ilegible para todo aquel que no conozca la clave mediante la cual ha sido cifrado.

– Proxy: ordenador, generalmente un servidor, intermedio usado en las comunicaciones entre otros dos equipos, siendo normalmente usado de manera trasparente para el usuario.

General:

– Ciberseguridad: la capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos.

– Ciberespacio: espacio virtual que engloba todos los sistemas TIC. El ciberespacio se apoya en la disponibilidad de Internet como red de redes, enriquecida con otras redes de transporte de datos.

– Redes y sistemas de información: se entiende por este concepto uno de los tres siguientes puntos:

• Las redes de comunicaciones electrónicas, tal y como vienen definidas en el número 31 del anexo II de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
• Todo dispositivo o grupo de dispositivos interconectados o relacionados entre sí en el que uno o varios de ellos realizan, mediante un programa, el tratamiento automático de datos digitales.
• Los datos digitales almacenados, tratados, recuperados o transmitidos mediante elementos contemplados anteriormente para su funcionamiento, utilización, protección y mantenimiento.

– Seguridad en redes y sistemas de información: la capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos.

– Operador de servicios esenciales: entidad pública o privada que se identifique considerando los factores establecidos en el artículo 6 del Real Decreto-ley 12/2018, de 7 de septiembre, que preste dichos servicios en alguno de los sectores estratégicos definidos en el anexo de la Ley 8/2011, de 28 de abril.

– Servicio digital: servicio de la sociedad de la información entendido en el sentido recogido en la letra a) del anexo de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

– Proveedor de servicios digitales: persona jurídica que presta un servicio digital.

– Ciberincidente: todo hecho que tenga efectos adversos reales en la seguridad de las redes y sistemas de información.

– Gestión de ciberincidentes: todos los procedimientos seguidos para detectar, analizar y limitar un incidente y responder ante este.

– Ciberamenaza: amenaza a los sistemas y servicios presentes en el ciberespacio o alcanzables a través de este.

– Taxonomía: clasificación u ordenación en grupos de objetos o sujetos que poseen unas características comunes.

– RGPD: Reglamento General de Protección de Datos, Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

– OpenPGP: estándar basado en el programa PGP, del inglés *Pretty Good Privacy*, cuya finalidad es proteger la información mediante el uso de criptografía de clave pública, así como facilitar la autenticación de documentos gracias a firmas digitales.

– *Webinject*: herramienta gratuita y de código abierto diseñada principalmente para automatizar la prueba de las aplicaciones y servicios *web*.

– Telnet: protocolo de red que permite acceder a otra máquina para manejarla remotamente como si estuviéramos sentados delante de ella.

– RDP (*Remote Desktop Protocol*): protocolo propietario que permite la comunicación en la ejecución de una aplicación entre un terminal y un servidor.

– VNC (*Virtual Network Computing*): programa de software libre basado en una estructura cliente-servidor que permite observar remotamente las acciones del ordenador servidor a través de un ordenador cliente.

– SNMP (*Simple Network Management Protocol*): protocolo de red utilizado para el intercambio de mensajes para la administración de dispositivos en red.

– Redis: motor de base de datos en memoria, basado en el almacenamiento en tablas de *hashes*.

– ICMP (*Internet Control Message Protocol*): protocolo de control de mensajes de Internet.

– Copia de seguridad limpia: punto de restauración de un sistema de la que se tiene la seguridad de no estar comprometida.

§ 13

Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia

Jefatura del Estado
«BOE» núm. 109, de 7 de mayo de 2002
Última modificación: 15 de junio de 2021
Referencia: BOE-A-2002-8628

JUAN CARLOS I

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente Ley.

EXPOSICIÓN DE MOTIVOS

La sociedad española demanda unos servicios de inteligencia eficaces, especializados y modernos, capaces de afrontar los nuevos retos del actual escenario nacional e internacional, regidos por los principios de control y pleno sometimiento al ordenamiento jurídico.

La actual regulación del Centro Superior de Información de la Defensa está contenida en una pluralidad de disposiciones, ninguna de ellas de rango legal, que han supuesto un esfuerzo de adecuación de sus estructuras y funcionamiento a los nuevos requerimientos de la sociedad y del Estado. Sin embargo, carecen de una regulación unitaria y sistemática y con el rango legal apropiado a la luz de la Constitución.

Sólo el estatuto de su personal fue diseñado por una norma con rango de Ley formal y desarrollado reglamentariamente.

Esta situación hace necesario abordar una nueva regulación de los servicios de inteligencia mediante una norma con rango de Ley, en la que se recojan de una forma unitaria y sistemática la naturaleza, objetivos, principios, funciones, aspectos sustanciales de su organización y régimen jurídico administrativo, así como los controles parlamentario y judicial, constituyendo éstos la esencia de su funcionamiento eficaz y transparente.

Esta Ley, inspirándose en el modelo de los países de nuestro entorno político y cultural, pretende, por tanto, dotar a los servicios de inteligencia de los instrumentos precisos para que puedan cumplir los objetivos que les asignen las disposiciones legales y reglamentarias.

Se crea el Centro Nacional de Inteligencia que sustituye al Centro Superior de Información de la Defensa y, dada la naturaleza y misiones que tendrá encomendadas, se configura como Organismo público especial de los previstos en la disposición adicional décima de la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado.

De esta forma, contará con la necesaria autonomía funcional para el cumplimiento de sus misiones, por lo que tendrá un régimen específico presupuestario, de contratación y de personal.

Respecto de este último, esta Ley contiene la habilitación necesaria para que el Gobierno pueda aprobar un estatuto, único y uniforme, para todo el personal que preste servicios en el Centro Nacional de Inteligencia, ya que, en caso contrario, dicho personal se regiría por legislaciones distintas dependiendo de su condición y relación con la Administración.

La principal misión del Centro Nacional de Inteligencia será la de proporcionar al Gobierno la información e inteligencia necesarias para prevenir y evitar cualquier riesgo o amenaza que afecte a la independencia e integridad de España, los intereses nacionales y la estabilidad del Estado de derecho y sus instituciones.

El Centro continuará adscrito al Ministerio de Defensa.

Esta adscripción adquiere un nuevo sentido a la luz de los nuevos retos que para los servicios de inteligencia se derivan de los llamados riesgos emergentes, que esta Ley afronta al definir las funciones del Centro. Sus objetivos, definidos por el Gobierno, serán aprobados anualmente por el Consejo de Ministros y se plasmarán en la Directiva de Inteligencia.

El Centro Nacional de Inteligencia funcionará bajo el principio de coordinación con los demás servicios de información del Estado español. A estos efectos, se crea la Comisión Delegada del Gobierno para Asuntos de Inteligencia, presidida por el Vicepresidente del Gobierno que designe su Presidente e integrada por el Ministro de Asuntos Exteriores, el Ministro de Defensa, el Ministro del Interior, el Ministro de Economía, el Secretario general de la Presidencia, el Secretario de Estado de Seguridad y el Secretario de Estado Director del Centro Nacional de Inteligencia.

Por primera vez, una Ley contempla de forma específica el principio del control parlamentario de las actividades del Centro Nacional de Inteligencia. Esta Ley, dentro del respeto a la autonomía parlamentaria, prevé que sea la Comisión que controla los créditos destinados a gastos reservados la que efectúe el control de las actividades del Centro, conociendo los objetivos que hayan sido aprobados por el Gobierno y un informe anual sobre el grado de cumplimiento de los mismos y de sus actividades. De acuerdo con la normativa parlamentaria, los miembros de esta Comisión son también los que conocen de los secretos oficiales.

El proyecto incluye aquellos aspectos de la regulación del Centro Nacional de Inteligencia que, conforme a la Constitución, no están reservados a Ley Orgánica. Es en la Ley Orgánica complementaria de la presente Ley donde se aborda el control previo de las actividades del Centro Nacional de Inteligencia.

Ambas Leyes deben ser interpretadas conjunta y sistemáticamente, ya que la adopción de las medidas que requieran autorización judicial previa deberá justificarse en el cumplimiento de las funciones que la presente Ley asigna al Centro Nacional de Inteligencia.

CAPÍTULO I

Disposiciones generales

Artículo 1. *El Centro Nacional de Inteligencia.*

El Centro Nacional de Inteligencia es el Organismo público responsable de facilitar al Presidente del Gobierno y al Gobierno de la Nación las informaciones, análisis, estudios o propuestas que permitan prevenir y evitar cualquier peligro, amenaza o agresión contra la independencia o integridad territorial de España, los intereses nacionales y la estabilidad del Estado de derecho y sus instituciones.

Artículo 2. *Principios.*

1. El Centro Nacional de Inteligencia se regirá por el principio de sometimiento al ordenamiento jurídico y llevará a cabo sus actividades específicas en el marco de las habilitaciones expresamente establecidas en la presente Ley y en la Ley Orgánica 2/2002, de 7 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia.

2. Sin perjuicio de la protección de sus actividades, la actuación del Centro Nacional de Inteligencia será sometida a control parlamentario y judicial en los términos que esta Ley y la Ley Orgánica reguladora del control judicial previo del Centro Nacional de Inteligencia determinan.

3. En el desarrollo de sus funciones, el Centro Nacional de Inteligencia actuará bajo los principios de eficacia, especialización y coordinación, de acuerdo con los objetivos de inteligencia definidos por el Gobierno.

Artículo 3. *Programación de objetivos.*

El Gobierno determinará y aprobará anualmente los objetivos del Centro Nacional de Inteligencia mediante la Directiva de Inteligencia, que tendrá carácter secreto.

Artículo 4. *Funciones del Centro Nacional de Inteligencia.*

Para el cumplimiento de sus objetivos, el Centro Nacional de Inteligencia llevará a cabo las siguientes funciones:

a) Obtener, evaluar e interpretar información y difundir la inteligencia necesaria para proteger y promover los intereses políticos, económicos, industriales, comerciales y estratégicos de España, pudiendo actuar dentro o fuera del territorio nacional.

b) Prevenir, detectar y posibilitar la neutralización de aquellas actividades de servicios extranjeros, grupos o personas que pongan en riesgo, amenacen o atenten contra el ordenamiento constitucional, los derechos y libertades de los ciudadanos españoles, la soberanía, integridad y seguridad del Estado, la estabilidad de sus instituciones, los intereses económicos nacionales y el bienestar de la población.

c) Promover las relaciones de cooperación y colaboración con servicios de inteligencia de otros países o de Organismos internacionales, para el mejor cumplimiento de sus objetivos.

d) Obtener, evaluar e interpretar el tráfico de señales de carácter estratégico, para el cumplimiento de los objetivos de inteligencia señalados al Centro.

e) Coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, garantizar la seguridad de las tecnologías de la información en ese ámbito, informar sobre la adquisición coordinada de material criptológico y formar al personal, propio o de otros servicios de la Administración, especialista en este campo para asegurar el adecuado cumplimiento de las misiones del Centro.

f) Velar por el cumplimiento de la normativa relativa a la protección de la información clasificada.

g) Garantizar la seguridad y protección de sus propias instalaciones, información y medios materiales y personales.

Artículo 5. *Actividades del Centro Nacional de Inteligencia.*

1. Las actividades del Centro Nacional de Inteligencia, así como su organización y estructura interna, medios y procedimientos, personal, instalaciones, bases y centros de datos, fuentes de información y las informaciones o datos que puedan conducir al conocimiento de las anteriores materias, constituyen información clasificada, con el grado de secreto, de acuerdo con lo dispuesto en la legislación reguladora de los secretos oficiales y en los Acuerdos internacionales o, en su caso, con el mayor nivel de clasificación que se contemple en dicha legislación y en los mencionados Acuerdos.

2. El Centro Nacional de Inteligencia mantendrá con el resto de las Administraciones públicas, cuando proceda, las relaciones de cooperación y coordinación necesarias para el mejor cumplimiento de sus misiones, de acuerdo con la legislación vigente en cada caso y preservando la protección legal de las actividades del Centro.

3. El Centro Nacional de Inteligencia podrá disponer y usar de medios y actividades bajo cobertura, pudiendo recabar de las autoridades legalmente encargadas de su expedición las identidades, matrículas y permisos reservados que resulten precisos y adecuados a las necesidades de sus misiones.

Asimismo, sus miembros dispondrán de documentación que les acredite, en caso de necesidad, como miembros del Centro, sin que ello exonere a la persona o entidad ante la

que se produzca la acreditación de la obligación de guardar secreto sobre la identidad de dicho personal. Las autoridades competentes ante las que comparezcan miembros del Centro Nacional de Inteligencia, por motivos relacionados con actividades del servicio, adoptarán las medidas necesarias para asegurar la protección de los datos personales, identidad y apariencia de aquéllos.

También dispondrán de licencia de armas, en función de las necesidades del servicio, de acuerdo con la normativa vigente.

4. Los miembros del Centro Nacional de Inteligencia no tendrán la consideración de agentes de la autoridad, con excepción de aquellos que desempeñen cometidos profesionales relacionados con la protección del personal del Centro y de las instalaciones del mismo.

5. Para el cumplimiento de sus funciones, el Centro Nacional de Inteligencia podrá llevar a cabo investigaciones de seguridad sobre personas o entidades en la forma prevista en esta Ley y en la Ley Orgánica reguladora del control judicial previo del Centro Nacional de Inteligencia. Para la realización de estas investigaciones podrá recabar de organismos e instituciones públicas y privadas la colaboración precisa.

CAPÍTULO II

De la organización y régimen jurídico

Artículo 6. *Comisión Delegada del Gobierno para Asuntos de Inteligencia.*

1. La Comisión Delegada del Gobierno para Asuntos de Inteligencia velará por la adecuada coordinación de todos los servicios de información e inteligencia del Estado para la formación de una comunidad de inteligencia.

2. **(Anulado).**

> Téngase en cuenta que se declara inconstitucional y nula la redacción dada al apartado 2 por la disposición final 2 del Real Decreto-ley 8/2020, de 17 de marzo. Ref. BOE-A-2020-3824, por Sentencia del TC 110/2021, de 13 de mayo. Ref. BOE-A-2021-10023
>
> ---
>
> Redacción anterior:
>
> "2. La Comisión estará presidida por el Vicepresidente del Gobierno que designe su Presidente e integrada por los Ministros de Asuntos Exteriores, Defensa, Interior y Economía, así como por el Secretario general de la Presidencia, el Secretario de Estado de Seguridad y el Secretario de Estado Director del Centro Nacional de Inteligencia, que actuará como Secretario."

3. No obstante lo dispuesto en el apartado anterior, podrán ser convocados a las reuniones de la Comisión los titulares de aquellos otros órganos superiores y directivos de la Administración General del Estado que se estime conveniente.

4. Corresponde a la Comisión Delegada:

a) Proponer al Presidente del Gobierno los objetivos anuales del Centro Nacional de Inteligencia que han de integrar la Directiva de Inteligencia.

b) Realizar el seguimiento y evaluación del desarrollo de los objetivos del Centro Nacional de Inteligencia.

c) Velar por la coordinación del Centro Nacional de Inteligencia, de los servicios de información de los Cuerpos y Fuerzas de Seguridad del Estado y los órganos de la Administración civil y militar.

Artículo 7. *Organización.*

1. El Centro Nacional de Inteligencia se adscribe orgánicamente al Ministerio de Defensa.

2. Su organización, régimen económico-presupuestario y de personal se desarrollará en régimen de autonomía funcional bajo la figura de Organismo público con personalidad jurídica propia y plena capacidad de obrar.

3. El Centro Nacional de Inteligencia se estructura en una Dirección, cuyo titular tendrá rango de Secretario de Estado, una Secretaría General y en las unidades que se determinen reglamentariamente.

Artículo 8. *Régimen jurídico.*

1. El personal que preste servicios en el Centro Nacional de Inteligencia, cualquiera que sea su procedencia, estará sometido a un mismo y único estatuto de personal que será aprobado por el Gobierno y en el que, de acuerdo con las funciones y naturaleza propias del Centro, se regularán, al menos, los siguientes extremos:

a) El proceso de selección del personal, que exigirá la superación de pruebas objetivas de acuerdo con los principios de mérito y capacidad.

b) El carácter temporal o permanente de la relación de servicios con el Centro Nacional de Inteligencia.

c) La estructura jerárquica del Centro Nacional de Inteligencia y las relaciones orgánicas y funcionales consiguientes.

d) Las medidas administrativas que garanticen la reserva sobre los aspectos de gestión de personal que afecten al funcionamiento del Centro.

No obstante lo anterior, el Centro podrá contratar otro personal con carácter laboral para atender sus necesidades de mantenimiento y funcionamiento no vinculadas con el ejercicio efectivo de las funciones que la presente Ley le encomiende. Este personal podrá ser sometido a las medidas de seguridad y control que se estimen necesarias de las que se prevean con carácter general en el estatuto del personal del Centro.

e) Los supuestos, las condiciones y los efectos en que el personal del Centro pueda pasar a desempeñar puestos de trabajo en las Administraciones Públicas, con reincorporación o no a su cuerpo o escala de procedencia en los casos que así corresponda.

f) El régimen de derechos y deberes que conjugará el de la función pública y el del personal sujeto a disciplina militar.

2. El Centro Nacional de Inteligencia elaborará anualmente un anteproyecto de presupuesto y lo elevará al Ministro de Defensa para remisión al Consejo de Ministros, que lo integrará en los Presupuestos Generales del Estado para su posterior remisión a las Cortes Generales.

3. El control de la gestión económico-financiera se efectuará con arreglo a lo dispuesto en la Ley General Presupuestaria para los Organismos públicos previstos en la disposición adicional décima de la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado. El Gobierno establecerá las peculiaridades necesarias que garanticen su autonomía e independencia funcional.

4. En su régimen patrimonial y de contratación podrá someterse al derecho privado.

5. Se autoriza al Centro Nacional de Inteligencia a disponer del 18 por 100 del total de los créditos del capítulo destinado a gastos corrientes en bienes y servicios de su Presupuesto de Gastos vigente en cada momento, en concepto de anticipo de caja fija, al objeto de poder atender los gastos periódicos o repetitivos de material no inventariable, mantenimiento y conservación, tracto sucesivo, indemnizaciones por razón del servicio y otros de similares características.

6. Se autoriza al Centro Nacional de Inteligencia a disponer del 2,5 por ciento del total de los créditos del capítulo de inversiones reales de su Presupuesto de Gastos vigente en cada momento, en concepto de anticipo de caja fija para las adquisiciones de material y servicios complementarios en el exterior.

Artículo 9. *Secretario de Estado Director del Centro Nacional de Inteligencia.*

1. El Secretario de Estado Director del Centro Nacional de Inteligencia será nombrado por Real Decreto a propuesta del Ministro de Defensa. El mandato será de cinco años, sin perjuicio de la facultad del Consejo de Ministros de proceder a su sustitución en cualquier momento.

2. Corresponde al Secretario de Estado Director del Centro Nacional de Inteligencia impulsar la actuación del Centro y coordinar sus unidades para la consecución de los objetivos de inteligencia fijados por el Gobierno, asegurar la adecuación de las actividades del Centro a dichos objetivos y ostentar la representación de aquél.

Asimismo, le corresponde:

a) Elaborar la propuesta de estructura orgánica del Centro Nacional de Inteligencia y nombrar y separar a los titulares de sus órganos directivos.

b) Aprobar el anteproyecto de presupuesto.

c) Mantener los procedimientos de relación necesarios para el desarrollo de las actividades específicas del Centro Nacional de Inteligencia, así como la celebración de los contratos y convenios con entidades públicas o privadas que sean precisos para el cumplimiento de sus fines.

d) Mantener y desarrollar, dentro del ámbito de su competencia, la colaboración con los servicios de información de las Fuerzas y Cuerpos de Seguridad del Estado, y los órganos de la Administración civil y militar, relevantes para los objetivos de inteligencia.

e) Ejercer las facultades que otorgue la legislación vigente a los Presidentes y Directores de Organismos públicos y las que les atribuyan las disposiciones de desarrollo.

f) Desempeñar las funciones de Autoridad Nacional de Inteligencia y Contrainteligencia y la dirección del Centro Criptológico Nacional.

g) Realizar cuantas otras funciones le sean atribuidas legal o reglamentariamente.

Artículo 10. *Secretario general del Centro Nacional de Inteligencia.*

1. El Secretario general del Centro Nacional de Inteligencia, con rango de Subsecretario, será nombrado por Real Decreto a propuesta del Ministro de Defensa, entre personas de reconocida experiencia y competencia profesional en el ámbito de la Inteligencia. Sustituirá al Director en los casos de ausencia, vacante o enfermedad.

2. El Secretario general del Centro Nacional de Inteligencia ejercerá las funciones que le otorgue el Real Decreto de estructura del Centro, y, en particular, las siguientes:

a) Apoyar y asistir al Director del Centro Nacional de Inteligencia en el ejercicio de sus funciones.

b) Establecer los mecanismos y sistemas de organización del Centro y determinar las actuaciones precisas para su actualización y mejora.

c) Dirigir el funcionamiento de los servicios comunes del Centro a través de las correspondientes instrucciones y órdenes de servicio.

d) Desempeñar la jefatura superior del personal del Centro, elaborar la propuesta de relación de puestos de trabajo y determinar los puestos vacantes a proveer durante cada ejercicio.

e) Las demás que legal o reglamentariamente se le encomienden.

CAPÍTULO III

Del control

Artículo 11. *Control parlamentario.*

1. El Centro Nacional de Inteligencia someterá al conocimiento del Congreso de los Diputados, en la forma prevista por su Reglamento, a través de la Comisión que controla los créditos destinados a gastos reservados, presidida por el Presidente de la Cámara, la información apropiada sobre su funcionamiento y actividades. El contenido de dichas sesiones y sus deliberaciones será secreto.

2. La citada Comisión del Congreso de los Diputados tendrá acceso al conocimiento de las materias clasificadas, con excepción de las relativas a las fuentes y medios del Centro Nacional de Inteligencia y a aquellas que procedan de servicios extranjeros u organizaciones internacionales en los términos establecidos en los correspondientes acuerdos y convenios de intercambio de la información clasificada.

3. Los miembros de la Comisión correspondiente estarán obligados, en los términos del Reglamento del Congreso de los Diputados, a guardar secreto sobre las informaciones y

documentos que reciban. Una vez examinados los documentos, serán reintegrados al Centro Nacional de Inteligencia para su debida custodia, sin que se puedan retener originales, copias o reproducciones.

4. La Comisión a que se refiere este artículo conocerá de los objetivos de inteligencia establecidos anualmente por el Gobierno y del informe que, también con carácter anual, elaborará el Director del Centro Nacional de Inteligencia de evaluación de actividades, situación y grado de cumplimiento de los objetivos señalados para el período anterior.

Artículo 12. *Control judicial previo.*

El control judicial previo del Centro Nacional de Inteligencia se llevará a cabo en la forma prevista en la Ley Orgánica reguladora del control judicial previo del Centro Nacional de Inteligencia, complementaria de la presente Ley.

Disposición adicional primera. *Naturaleza jurídica.*

El Centro Nacional de Inteligencia queda incluido dentro de los Organismos públicos a que se refiere la disposición adicional décima de la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado.

Disposición adicional segunda. *Supresión del Centro Superior de Información de la Defensa.*

1. Queda suprimido el Centro Superior de Información de la Defensa.

2. El Centro Nacional de Inteligencia sucederá al Centro Superior de Información de la Defensa en el ejercicio de sus funciones y cometidos, quedando subrogado en la titularidad de los bienes, derechos y obligaciones del Estado afectos o constituidos en virtud de las mencionadas funciones y de su fondo documental.

3. Todas las referencias que contengan las disposiciones normativas vigentes al Centro Superior de Información de la Defensa, se entenderán hechas al Centro Nacional de Inteligencia.

Disposición adicional tercera. *Habilitación de adscripción orgánica.*

Se autoriza al Presidente del Gobierno para modificar, por Real Decreto, la adscripción orgánica del Centro Nacional de Inteligencia, prevista en el artículo 7.1 de esta Ley. El Departamento al que se adscriba el Centro ejercerá las competencias que, en relación con el mismo, atribuye esta Ley al Ministerio de Defensa y a su titular.

Disposición transitoria única. *Garantía de derechos adquiridos.*

1. El personal que, a la entrada en vigor de la presente Ley, tenga la consideración de personal estatutario permanente o temporal del Centro Superior de Información de la Defensa, quedará integrado en la misma condición en el Centro Nacional de Inteligencia.

2. En tanto no se produzca el desarrollo reglamentario de esta Ley y se apruebe un estatuto de personal del Centro Nacional de Inteligencia, continuará en vigor el Real Decreto 1324/1995, de 28 de julio, por el que se establece el estatuto de personal del Centro Superior de Información de la Defensa.

3. El grupo de clasificación, grado personal y demás derechos económicos que el personal del Centro Superior de Información de la Defensa tuviera reconocidos, quedarán plenamente garantizados en el nuevo régimen de personal.

Disposición derogatoria única.

Quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en la presente Ley.

Disposición final primera. *Facultad de desarrollo.*

Se faculta al Consejo de Ministros para dictar cuantas disposiciones sean necesarias para la aplicación y desarrollo de la presente Ley.

Disposición final segunda. *Modificaciones presupuestarias.*

El Ministerio de Hacienda realizará las modificaciones presupuestarias oportunas para dar cumplimiento a lo dispuesto en la presente Ley.

Disposición final tercera. *Entrada en vigor.*

La presente Ley entrará en vigor el mismo día de su publicación en el "Boletín Oficial del Estado".

§ 14

Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia

Jefatura del Estado
«BOE» núm. 109, de 7 de mayo de 2002
Última modificación: sin modificaciones
Referencia: BOE-A-2002-8627

JUAN CARLOS I

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente Ley Orgánica.

EXPOSICIÓN DE MOTIVOS

La presente Ley Orgánica es complementaria de la Ley 11/2002, de 7 de mayo, reguladora del Centro Nacional de Inteligencia, y modifica la Ley Orgánica del Poder Judicial, a los efectos de establecer un control judicial de las actividades del citado Centro que afecten a los derechos fundamentales reconocidos en el artículo 18.2 y 3 de la Constitución española.

Para las actividades que puedan afectar a la inviolabilidad del domicilio y al secreto de las comunicaciones, la Constitución española exige en su artículo 18 autorización judicial, y el artículo 8 del Convenio Europeo para Protección de los Derechos Humanos y de las Libertades Fundamentales exige que esta injerencia esté prevista en la Ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.

A estos efectos, esta Ley Orgánica, cuyo alcance resulta de una interpretación conjunta con la Ley reguladora del Centro Nacional de Inteligencia, determina tanto la forma de nombramiento de un Magistrado del Tribunal Supremo específicamente encargado del control judicial de las actividades del Centro Nacional de Inteligencia, como el procedimiento conforme al cual se acordará o no la autorización judicial necesaria para dichas actividades. El plazo para acordarlas será ordinariamente de setenta y dos horas, pudiendo reducirse, de forma extraordinaria y por motivos de urgencia debidamente justificados, a veinticuatro horas.

Artículo único. *Control judicial previo del Centro Nacional de Inteligencia.*

1. El Secretario de Estado Director del Centro Nacional de Inteligencia deberá solicitar al Magistrado del Tribunal Supremo competente, conforme a la Ley Orgánica del Poder Judicial, autorización para la adopción de medidas que afecten a la inviolabilidad del domicilio y al secreto de las comunicaciones, siempre que tales medidas resulten necesarias para el cumplimiento de las funciones asignadas al Centro.

2. La solicitud de autorización se formulará mediante escrito que contendrá los siguientes extremos:

a) Especificación de las medidas que se solicitan.

b) Hechos en que se apoya la solicitud, fines que la motivan y razones que aconsejan la adopción de las medidas solicitadas.

c) Identificación de la persona o personas afectadas por las medidas, si fueren conocidas, y designación del lugar donde hayan de practicarse.

d) Duración de las medidas solicitadas, que no podrá exceder de veinticuatro horas en el caso de afección a la inviolabilidad del domicilio y tres meses para la intervención o interceptación de las comunicaciones postales, telegráficas, telefónicas o de cualquier otra índole, ambos plazos prorrogables por sucesivos períodos iguales en caso de necesidad.

3. El Magistrado acordará, mediante resolución motivada en el plazo improrrogable de setenta y dos horas, la concesión o no de la autorización solicitada. Dicho plazo se reducirá a veinticuatro horas, por motivos de urgencia debidamente justificados en la solicitud de autorización del Secretario de Estado Director del Centro Nacional de Inteligencia que, en todo caso, contendrá los extremos especificados en el apartado anterior de este artículo.

El Magistrado dispondrá lo procedente para salvaguardar la reserva de sus actuaciones, que tendrán la clasificación de secreto.

4. El Secretario de Estado Director del Centro Nacional de Inteligencia ordenará la inmediata destrucción del material relativo a todas aquellas informaciones que, obtenidas mediante la autorización prevista en este artículo, no guarden relación con el objeto o fines de la misma.

Disposición adicional única. *Modificación de la Ley Orgánica del Poder Judicial.*

1. Se modifica el artículo 125 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, que tendrá la siguiente redacción:

> «125. El Presidente del Consejo General del Poder Judicial tendrá las siguientes funciones:
>
> 1. Ostentar la representación del Consejo General del Poder Judicial.
> 2. Convocar y presidir las sesiones del Pleno y de la Comisión Permanente, decidiendo los empates con voto de calidad.
> 3. Fijar el orden del día de las sesiones del Pleno y de la Comisión Permanente.
> 4. Someter cuantas propuestas considere oportunas en materias de la competencia del Pleno o de la Comisión Permanente.
> 5. Someter al Pleno las propuestas de nombramiento de los Magistrados del Tribunal Supremo a que se refiere el artículo 127.4) de esta Ley.
> 6. Proponer el nombramiento de Ponencias para preparar la resolución o despacho de un asunto.
> 7. Autorizar con su firma los acuerdos del Pleno y de la Comisión Permanente.
> 8. Ejercer la superior dirección de las actividades de los órganos técnicos del Consejo.
> 9. Las demás previstas en la Ley.»

2. Se modifica el artículo 127 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, que tendrá la siguiente redacción:

> «127. Será de la competencia del Pleno del Consejo General del Poder Judicial:

1. La propuesta de nombramiento por mayoría de 3/5 del Presidente del Tribunal Supremo y del Consejo General del Poder Judicial y del Vicepresidente de este último.

2. La propuesta de nombramiento de miembros del Tribunal Constitucional, que habrá de ser adoptada por mayoría de 3/5 de sus miembros.

3. La propuesta de nombramiento de Presidentes de Sala y Magistrados del Tribunal Supremo y cualesquiera otros discrecionales.

4. La propuesta de nombramiento del Magistrado de la Sala Segunda de lo Penal o Tercera de lo Contencioso-Administrativo, del Tribunal Supremo, competente para conocer de la autorización de las actividades del Centro Nacional de Inteligencia que afecten a los derechos fundamentales reconocidos en el artículo 18.2 y 3 de la Constitución, así como la propuesta de nombramiento del Magistrado de dichas Salas del Tribunal Supremo que lo sustituya en caso de vacancia, ausencia o imposibilidad.

5. La propuesta de nombramiento de Presidente de los Tribunales Superiores de Justicia de las Comunidades Autónomas.

6. Evacuar la audiencia prevista en el artículo 124.4 de la Constitución sobre nombramiento del Fiscal General del Estado.

7. Resolver los recursos de alzada interpuestos contra los acuerdos de la Comisión Permanente, de la Comisión Disciplinaria y de las Salas de Gobierno de los Tribunales Superiores de Justicia y de los órganos de gobierno de los Tribunales y Juzgados.

8. Resolver los expedientes de rehabilitación instruidos por la Comisión Disciplinaria.

9. Evacuar los informes previstos en la Ley y ejercer la potestad reglamentaria atribuida por la Ley al Consejo General del Poder Judicial.

10. Acordar, en los casos legalmente establecidos, la separación y jubilación de los Jueces y Magistrados en los supuestos no previstos en el artículo 131.3.

11. Elegir y nombrar los Vocales componentes de las Comisiones y Delegaciones.

12. Aprobar la memoria anual que con motivo de la apertura del año judicial leerá su Presidente sobre el estado de la Administración de Justicia.

13. Elaborar el Presupuesto del Consejo General del Poder Judicial que se integrará en los Generales del Estado, en una sección independiente.

14. Dirigir la ejecución del presupuesto del Consejo y controlar su cumplimiento.

15. Cualesquiera otras funciones que correspondan al Consejo General del Poder Judicial y no se hallen expresamente atribuidas a otros órganos del mismo.»

3. Se modifica el artículo 135 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, que tendrá la siguiente redacción:

«135. Corresponderá a la Comisión de calificación informar, en todo caso, sobre los nombramientos de la competencia del Pleno, excepto el nombramiento del Magistrado del Tribunal Supremo previsto en el artículo 127.4) de esta Ley.»

4. Se añade un nuevo artículo 342 bis a la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, que tendrá la siguiente redacción:

«Artículo 342 bis.

El Magistrado del Tribunal Supremo competente para conocer de la autorización de las actividades del Centro Nacional de Inteligencia que afecten a los derechos fundamentales reconocidos en el artículo 18.2 y 3 de la Constitución se nombrará por un período de cinco años, a propuesta del Consejo General del Poder Judicial, entre Magistrados de dicho Tribunal que cuenten con tres años de servicios en la categoría.»

Disposición final única. *Entrada en vigor.*

La presente Ley Orgánica entrará en vigor el mismo día de su publicación en el «Boletín Oficial del Estado».

§ 15

Ley 9/1968, de 5 de abril, sobre secretos oficiales

Jefatura del Estado
«BOE» núm. 84, de 6 de abril de 1968
Última modificación: 11 de octubre de 1978
Referencia: BOE-A-1968-444

Es principio general, aun cuando no esté expresamente declarado en nuestras Leyes Fundamentales, la publicidad de la actividad de los Órganos del Estado, porque las cosas públicas que a todos interesan pueden y deben ser conocidas de todos.

Este principio de publicidad en mayor o menor extensión, se halla regulado en lo que concierne a los debates e interpelaciones en las Cortes Españolas y al despacho de los asuntos judiciales, pero, en cambio, sólo de una manera fraccionada tiene su regulación, en lo que atañe a la Administración del Estado, en dispersas disposiciones, entre las que, por su reciente promulgación, pueden citarse la Ley de Prensa (artículo séptimo) y Decreto setecientos cincuenta/mil novecientos sesenta y seis, de treinta y uno de marzo, en las que sólo se contempla la publicidad en el aspecto parcial de la información debida a las publicaciones periódicas y agencias de información. Una regulación suficiente existe en la esfera de la Administración Local.

Mas si la publicidad ha de ser característica de la actuación de los Órganos del Estado, es innegable la necesidad de imponer limitaciones, cuando precisamente de esa publicidad puede derivarse perjuicio para la causa pública, la seguridad del mismo Estado o los intereses de la colectividad nacional.

Destancan por su especial importancia aquellas cuestiones cuyo conocimiento por personas no autorizadas pueda dañar o ponga en riesgo la seguridad del Estado o los intereses fundamentales de la Nación y que constituyen los verdaderos «secretos oficiales», protegidos por sanciones penales que, tanto en el Código Penal Común como en el de Justicia Militar, alcanzan penas de la máxima severidad. Pero esta sanción penal, especialmente represiva, sólo de una manera indirecta, por medio de la intimidación, protege el descubrimiento o revelación de secretos. Las medidas de protección eficaces son las que la propia Administración ha de establecer para garantizar que los documentos o materiales en que físicamente se reflejan los secretos, no puedan ser conocidos más que por aquellas personas que, por razón de su cometido, estén autorizadas para ello.

En este aspecto existe una laguna en nuestra legislación, que, al contrario de lo que ocurre en los Estados caracterizados por la mayor libertad de información, no prevé una regulación de las medidas protectoras de los secretos oficiales Para remediar esta situación, la Ley establece un conjunto de medidas positivas para evitar que trascienda el conocimiento de lo que debe permanecer secreto, señalando normas severas que impidan la generalización de calificaciones que tienen carácter excepcional.

Con la denominación de «materias clasificadas» también utilizada en otros países, se comprenden los dos grados de secretos oficiales generalmente admitidos. La determinación

de las Autoridades y funcionarios que pueden otorgar y levantar las calificaciones, los efectos de cada una de éstas y las líneas generales de las medidas protectoras que habrán de desarrollarse reglamentariamente y con carácter uniforme por todos los servicios afectados, constituyen el contenido fundamental de la Ley, que se completa con un sistema de protección, así como la referencia de las responsabilidades que procedan por infracciones en materia de secretos oficiales.

Asimismo, desde el punto de vista de la seguridad jurídica y de la garantía de los ciudadanos, es importante resaltar que la Ley establece la necesidad de notificar a los medios de información la declaración de «materia clasificada» cuando se prevea que ésta puede llegar a conocimiento de ellos, así como la circunstancia de que conste el hecho de la clasificación para que recaiga sobre los particulares la obligación de colaboración que impone el artículo nueve, uno. Y, en fin, se consagra la expresa admisión de recurso contencioso-administrativo contra las resoluciones sancionadoras que pongan fin a la vía administrativa, sin olvidar por lo demás el importante juego del control político que en esta materia se reconoce a las Cortes Españolas y al Consejo Nacional del Movimiento.

En su virtud, y de conformidad con la Ley aprobada por las Cortes Españolas, vengo en sancionar:

Artículo primero.

Uno. Los Órganos del Estado estarán sometidos en su actividad al principio de publicidad, de acuerdo con las normas que rijan su actuación, salvo los casos en que por la naturaleza de la materia sea ésta declarada expresamente «clasificada», cuyo secreto o limitado conocimiento queda amparado por la presente Ley.

Dos. Tendrán carácter secreto, sin necesidad de previa clasificación, las materias así declaradas por Ley.

Artículo segundo.

A los efectos de esta Ley podrán ser declaradas "materias clasificadas" los asuntos, actos, documentos, informaciones, datos y objetos cuyo conocimiento por personas no autorizadas pueda dañar o poner en riesgo la seguridad y defensa del Estado.

Artículo tercero.

Las «materias clasificadas» serán calificadas en las categorías de secreto y reservado en atención al grado de protección que requieran.

Artículo cuarto.

La calificación a que se refiere el artículo anterior corresponderá exclusivamente, en la esfera de su competencia, al Consejo de Ministros y a la Junta de Jefes de Estado Mayor.

Artículo quinto.

La facultad de calificación a que se refiere el artículo anterior no podrá ser transferida ni delegada.

Artículo sexto.

El personal de la Administración del Estado o de las Fuerzas Armadas que tenga conocimiento de cualquier asunto que, a su juicio, reúna las condiciones del artículo segundo, deberá hacerlo llegar a alguno de los órganos comprendidos en el artículo cuarto en la forma que reglamentariamente se determine.

Artículo séptimo.

La cancelación de cualquiera de las calificaciones previstas en el artículo tercero de esta Ley será dispuesta por el órgano que hizo la respectiva declaración.

Artículo octavo.

Las calificaciones de secreto o reservado, hechas con arreglo a los términos de la presente Ley y de las disposiciones que reglamentariamente se dicten para su aplicación, determinarán, entre otros, los siguientes efectos:

A) Solamente podrán tener conocimiento de las "materias clasificadas" los órganos y las personas debidamente facultadas para ello y con las formalidades y limitaciones que en cada caso se determinen.

B) La prohibición de acceso y las limitaciones de circulación a personas no autorizadas en locales, lugares o zonas en que radiquen las «materias clasificadas».

C) El personal que sirva en la Administración del Estado y en las Fuerzas Armadas estará obligado a cumplir cuantas medidas se hallen previstas para proteger las «materias clasificadas».

Artículo noveno.

Uno. La persona a cuyo conocimiento o poder llegue cualquier «materia clasificada», conforme a esta Ley, siempre que le conste esta condición, está obligada a mantener el secreto y entregarla a la Autoridad civil o militar más cercana y, si ello no fuese posible, a poner en conocimiento de ésta su descubrimiento o hallazgo. Esta Autoridad lo comunicará sin dilación al Departamento ministerial que estime interesado o a la Presidencia del Gobierno, adoptando entretanto las medidas de protección que su buen juicio le aconseje.

Dos. Cuando una «materia clasificada» permita prever que pueda llegar a conocimiento de los medios de información, se notificará a éstos la calificación de secreto o reservado.

Artículo diez.

Uno. Las calificaciones a que se refiere el artículo cuarto, en cualquiera de sus grados, se conferirán mediante un acto formal y con los requisitos y materializaciones que reglamentariamente se determinen.

Dos. La declaración de "materias clasificadas" no afectará al Congreso de los Diputados ni al Senado, que tendrán siempre acceso a cuanta información reclamen, en la forma que determinen los respectivos Reglamentos y, en su caso, en sesiones secretas.

Tres. Las «materias clasificadas» llevarán consigo una anotación en la que conste esta circunstancia y la calificación que les corresponda conforme al artículo tercero.

Cuatro. Las copias o duplicados de una «materia clasificada» tendrán el mismo tratamiento y garantía que el original y sólo se obtendrán previa autorización especial y bajo numeración.

Artículo once.

Uno. Las personas facultadas para tener acceso a una «materia clasificada» quedarán obligadas a cumplir con las medidas y prevenciones de protección que reglamentariamente se determinen, así como las particulares que para cada caso concreto puedan establecerse.

Dos. Corresponde a los órganos señalados en el artículo cuarto conceder en sus respectivas dependencias las autorizaciones para el acceso a las "materias clasificadas", así como para su desplazamiento fuera de las mismas.

Tres. A toda persona que tenga acceso a una «materia clasificada» se le hará saber la índole de la misma con las prevenciones oportunas.

Artículo doce.

Los órganos referidos en el artículo cuarto atenderán al mantenimiento y mejora de los sistemas de protección y velarán por el efectivo cumplimiento de cuanto se dispone en la presente Ley y en especial por la correcta aplicación de las calificaciones de secreto o reservado y porque se promuevan las acciones penales, las medidas disciplinarias y los expedientes administrativos para corregir las infracciones a esta Ley.

Artículo trece.

Las actividades reservadas por declaración de Ley y las "materias clasificadas" no podrán ser comunicadas, difundidas ni publicadas, ni utilizado su contenido fuera de los límites establecidos por la Ley. El incumplimiento de esta limitación será sancionado, si procediere, conforme a las Leyes penales, y por vía disciplinaria, en su caso, considerándose en este último supuesto la infracción como falta muy grave.

Artículo catorce.

La calificación de secreto o reservado no impedirá el exacto cumplimiento de los trámites de audiencia, alegaciones, notificaciones directas a los interesados, sin perjuicio de la eventual aplicación de las sanciones previstas en esta Ley en caso de violación del secreto por parte de los interesados.

DISPOSICIÓN FINAL

En Reglamento único, de aplicación general a toda la Administración del Estado y a las Fuerzas Armadas, se regularán los procedimientos y medidas necesarios para la aplicación de la presente Ley y protección de las «materias clasificadas».

Se determinará igualmente con todo el detalle necesario y con especificación de las medidas técnicas precisas el régimen de custodia, traslado, registro, archivo, examen y destrucción de las materias clasificadas, así como la elaboración de copias o duplicados de tales materias.

También se dispondrá lo necesario para que el personal de la Administración Civil del Estado y de las Fuerzas Armadas se halle debidamente instruido en cuestiones de seguridad y protección de secretos.

§ 16

Decreto 242/1969, de 20 de febrero, por el que se desarrollan las disposiciones de la Ley 9/1968, de 5 de abril sobre Secretos Oficiales

Presidencia del Gobierno
«BOE» núm. 47, de 24 de febrero de 1969
Última modificación: sin modificaciones
Referencia: BOE-A-1969-263

La disposición final de la Ley nueve/mil novecientos sesenta y ocho, de cinco de abril, dispone que en el Reglamento único, de aplicación general a toda la Administración del Estado y a las Fuerzas Armardas, se regularán los procedimientos y medidas necesarias para la aplicación de la Ley y protección de las «materias clasificadas».

Para lograr una unificación normativa internacional y tener el mismo grado de protección a las materias clasificadas en los distintos países parece aconsejable utilizar las enseñanzas del derecho comparado, en especial el de las naciones muy industrializadas con mayor experiencia en la información tecnológica.

De acuerdo con la expresada tendencia se ha recogido en este Reglamento lo relativo a definiciones, materias clasificadas, violaciones de su protección, Servicio de Protección de Materias Clasificadas y otros particulares necesarios para la adecuada aplicación de la Ley antes mencionada.

En su virtud, a propuesta del Vicepresidente del Gobierno, de conformidad con el Consejo de Estado y previa deliberación del Consejo de Ministros en su reunión del día cinco de febrero de mil novecientos sesenta y nueve.

DISPONGO:

Artículo primero.

De acuerdo con lo dispuesto en el artículo primero de la Ley nueve/mil novecientos sesenta y ocho, de cinco de abril, los Órganos del Estado estarán sometidos en el ejercicio de su actividad al principio de publicidad, salvo en las materias que tengan por Ley el carácter de secretas o en aquellas otras que, por su naturaleza, sean expresamente declaradas como «clasificadas».

Artículo segundo. *Definiciones.*

A efectos de lo dispuesto en el artículo segundo de la Ley podrá entenderse:

Uno. Por asuntos, todos los temas que se refieran a las materias que en el mismo se especifican.

Dos. Por acto, cualquier manifestación o acuerdo de la vida político-administrativa tendente a la obtención de fines específicos.

Tres. Por documentos, cualquier constancia gráfica o de cualquier otra naturaleza y muy especialmente:

a) Los impresos, manuscritos, papeles mecanografiados o taquigrafiados y las copias de los mismos, cualesquiera sean los procedimientos empleados para su reproducción: los planos, proyectos, esquemas, esbozos, diseños, bocetos, diagramas, cartas, croquis y mapas de cualquier índole, ya lo sean en su totalidad, ya las partes o fragmentos de los mismos.

b) Las fotografías y sus negativos, las diapositivas, los positivos y negativos de película, impresionable por medio de cámaras cinematográficas y sus reproducciones.

c) Las grabaciones sonoras de todas clases.

d) Las planchas, moldes, matrices, composiciones tipográficas, piedras litográficas, grabados en película cinematográfica, bandas escritas o perforadas, la memoria transitorizada de un cerebro electrónico y cualquier otro material usado para reproducir documentos.

Cuatro. Por informaciones, los conocimientos de cualquier clase de asuntos o los comprendidos como materias clasificadas en el citado artículo segundo de la Ley.

Cinco. Por datos y objetos, los antecedentes necesarios para el conocimiento completo o Incompleto de las materias clasificadas, las patentes, las materias primas y los productos elaborados, el utillaje, cuños, matrices y sellos de todas clases, así como los lugares, obras, edificios e Instalaciones de interés para la defensa nacional o la investigación científica.

Seis. Se entenderá también como materias propias de este Decreto, todas aquellas que, sin estar enumeradas en el presente artículo, por su naturaleza, puedan ser calificadas de asunto, acto, documento, información, dato u objeto, de acuerdo con lo dispuesto en el artículo dos de la Ley.

Artículo tercero. *Materias clasificadas de «secreto» y de «reservado».*

I. La clasificación de «secreto» se aplicará a todas las materias referidas en el artículo anterior que precisen del más alto grado de protección por su excepcional importancia y cuya revelación no autorizada por autoridad competente para ello, pudiera dar lugar a riesgos o perjuicios de la seguridad del Estado, o pudiera comprometer los Intereses fundamentales de la Nación en materia referente a la defensa nacional, la paz exterior o el orden constitucional.

II. La clasificación de «reservado» se aplicará a tos asuntos, actos, documentos, informaciones, datos y objetos no comprendidos en el apartado anterior por su menor importancia, pero cuyo conocimiento o divulgación pudiera afectar a los referidos intereses fundamentales de la Nación, la seguridad del Estado, la defensa nacional, la paz exterior o el orden constitucional.

III. Siempre que ello sea posible, la autoridad encargada de la calificación indicará el plazo de duración de ésta, con mención de si pudiera ser suprimida o rebajada de grado. Para ello, podrá fijar una fecha o indicar un acontecimiento o hecho límite de dicho plazo. Tal indicación no deberá incluirse en el texto, sino que constará en una anotación, anterior o posterior, al mismo.

De la misma manera, la citada Autoridad, en el momento de verificar la clasificación, señalará del personal a sus órdenes, aquellos que puedan tener acceso a las materias «secretas» o «reservadas», indicando, en cada caso, las formalidades y limitaciones que sean necesarias para el cumplimiento de esta clasificación.

IV. A efectos de evitar la acumulación excesiva de material calificado, la autoridad encargada de la calificación deberá señalar los procedimientos para determinar, periódicamente, la conveniencia de la reclasificación o desclasificación de aquel material.

Artículo cuarto. *Violaciones de la protección de las materias clasificadas.*

Cualquier persona que preste sus servicios en la Administración del Estado o en las Fuerzas Armadas, sea cual fuere su situación, que tenga conocimiento de cualquier asunto que, a su juicio, reúna las condiciones de «secreto» o «reservado», o conozca de la revelación a persona no autorizada de materias clasificadas, o compruebe el extravío de cualquier documento o material clasificado, deberá poner estos hechos, inmediatamente, en

conocimiento de su Jefe inmediato. Este Jefe, siguiendo el proceso reglamentario más rápido, lo pondrá, igualmente, en conocimiento del Jefe del Servicio de Protección de Materias Clasificadas del Ministerio en el cual preste sus servicios, en su defecto, del Director general o autoridad equivalente del Organismo al cual la materia de referencia estuviera confiada o de aquel a quien afectare la revelación de información o el extravío del documento o material de referencia.

Artículo quinto.

Si en un Organismo, Entidad o Servicio, sea Autoridad encargada de hacer la calificación, sea depositario de materias clasificadas, se comprobase una revelación no autorizada o el extravío de documentos o material, la máxima jerarquía de aquéllos deberá ordenar se proceda, con carácter de máxima urgencia, a hacer las averiguaciones pertinentes, tanto para fijar las responsabilidades a que hubiere lugar, que habrán de atribuirse, siempre que sea posible, a persona determinada individualmente y no al cargo o función que desempeñare, como para la recuperación del documento o material extraviado.

Artículo sexto.

Si el extravío, o la revelación de información, correspondiese a una materia con la calificación de «secreto», el Director general o autoridad equivalente, comunicará, inmediatamente, tal hecho al Servicio de Protección de Materias Clasificadas del Ministerio correspondiente.

Si se tratase de una materia con calificación de «reservado», deberá ordenar se proceda a registrar su falta en el archivo o depósito correspondiente, si lo hubiere, y a adoptar las medidas pertinentes para su recuperación y esclarecimiento

Artículo séptimo.

La apreciación y decisión con carácter definitivo, en relación con las actuaciones investigadoras referidas en el artículo quinto, corresponderán, en todo caso, y oído el Servicio de Protección de Materias Clasificadas correspondiente, al Ministro del Departamento de que se trate.

Artículo octavo.

En caso de extravío de documentación o material, y si fuere encontrada la materia clasificada, el Director general o autoridad equivalente, deberá comunicar tal hecho al Servicio de Protección de Materias Clasificadas aportando tanto los datos suficientes que permitan su correcta identificación, cuanto los pormenores relativos a la circunstancia del hallazgo.

Artículo noveno. *Servicio de Protección de Materias Clasificadas.*

Los Servicios de Protección de Materias Clasificadas de los Departamentos ministeriales, que tendrán la consideración de Unidades Centrales en aquellos casos en que así se precise, o de Dependencias afectas directamente al despacho de los Ministros respectivos y que estarán a cargo de funcionarios de su libre designación, deberán:

a) Asegurar el adecuado tratamiento de las materias clasificadas, tanto si se han producido en el Departamento como si se han recibido en el mismo procedentes de otras dependencias de la Administración.

b) Instruir convenientemente respecto de las normas de protección al personal que tenga acceso, fehacientemente autorizado, al material clasificado,

c) Elaborar las condiciones de seguridad privativas del Ministerio, de las cuales deberán tener constancia, junto con las disposiciones necesarias para asegurar el perfecto cumplimiento de lo establecido en este Decreto, las Entidades y personas del propio Ministerio con competencia para la declaración de materias clasificables, según se dispone en el artículo cuarto de la Ley.

d) Responder en todo tiempo, de la mejor protección del material calificado que se le entregue para su custodia y, especialmente, de cerrar bajo seguro el material calificado de

«secreto» en instalación de seguridad apropiada, siempre que la misma no esté en uso o bajo supervisión directa de funcionarios autorizados.

e) Establecer procedimientos adecuados tendentes a evitar que personas no autorizadas puedan tener acceso, sea visual, sea auditivo, a información o material secreto, no discutiéndose con o en presencia de personas no autorizadas, el contenido de aquéllos.

f) Mantener el control o registro de las materias clasificadas.

Artículo diez. *Funcionarios del Servicio de Protección de Materias Clasificadas.*

El cumplimiento de las medidas de protección deberá constituir parte principal de la tarea o función de cada uno de los funcionarios adscritos a los Servicios de Protección de Materias Clasificadas y no un cometido accesorio.

Artículo once. *Requisitos formales de la clasificación.*

El acto formal de clasificación habrá de ajustarse a los siguientes requisitos:

A) Si se trata de calificación otorgada por autoridades legitimadas para ello por el número uno del artículo cuarto de la Ley, en el documento origen de aquélla deberá hacerse constar la autoridad que la atribuya, la declaración constitutiva de materia clasificada, el ámbito a que se refiere según se dispone en el artículo segundo de la Ley, el lugar, fecha, sello y firma entera o abreviada de aquélla. Una diligencia se adherirá a la materia clasificada, la cual comprenderá todos los aspectos que dicho documento comprende.

B) En el caso de tratarse de la clasificación provisional a que se refiere el número dos del referido artículo cuarto de la Ley, la autoridad que la proponga deberá especificar los mismos requisitos anteriores y añadirá una explicación razonada del porqué de la misma. Dentro del plazo legal al efecto establecido, la autoridad competente, según lo dispuesto en el número uno del artículo de referencia, antes de proceder a la firma o aprobación de la calificación propuesta, comprobara si su contenido corresponde con las definiciones establecidas en los párrafos I y II del artículo tercero de este Decreto, con especificación de los requisitos señalados en el párrafo anterior. Caso de no existir justificación, promoverán que dicha calificación provisional sea disminuida o desechada.

C) En el caso de que partes destacadas de documentos o material exijan la calificación de secreto, y existan otras a las cuales pudiera corresponder calificación inferior, cada una de dichas partes será clasificada de acuerdo con su contenido, pero el documento o material en su conjunto, ostentará la calificación más elevada, haciéndose constar así en el documento que atribuya la calificación.

D) Si tales documentos o material son trasladados a Entidades u Organismos distintos del de origen, aparte los datos anteriores, deberán especificar en la notificación escrita de la calificación atribuida lo siguiente: «Este material contiene información relativa a secretos oficiales, según lo dispuesto en la Ley nueve/mil novecientos sesenta y ocho de cinco de abril».

E) La información de defensa de naturaleza reservada, suministrada a España por un país extranjero o por una Organización internacional, recibirá una clasificación que asegure un grado de protección equivalente o mayor que el requerido por el Gobierno u Organismo internacional que suministró la información.

F) La notificación de la calificación a que se refiere el número dos del artículo noveno de la Ley se efectuará por conducto del Director general de Prensa, en la forma establecida en la Ley de Procedimiento Administrativo.

Artículo doce. *Lugares para la custodia y salvaguardia del material clasificado.*

La posesión o uso de información o material clasificado como secreto estará limitada a lugares donde se disponga de instalaciones para su almacenaje y segura protección, y a los cuales no pueden tener acceso otras personas que no sean las que, de manera fehaciente, hayan sido autorizadas para ello por las autoridades señaladas en el artículo cuarto de la Ley.

Artículo trece. *Custodia del material clasificado como «secreto».*

Por lo menos, los documentos, información y material clasificado de «secreto», estará guardado en una caja fuerte o armario-archivador a prueba de incendios y dotados de cerraduras de combinación de disco, cuyas dimensiones, peso, construcción e instalación hagan mínimas las posibilidades de robo, violación e indiscreciones.

De ser ello necesario, por el volumen total del material clasificado, podrán habilitarse salas o sótanos aprobados al efecto por la persona responsable del Servicio de Protección de Materias Clasificadas que impliquen unas condiciones, cuando menos, similares a los sistemas indicados en el apartado anterior.

Si no fuere posible disponer de las instalaciones especificadas en los párrafos anteriores, las materias clasificadas de «secreto» deberán estar protegidas por una guardia armada.

Artículo catorce. *Custodia del material clasificado como «reservado».*

Como mínimo, los documentos, información y material clasificados de «reservado» deberán ser almacenados en la forma especificada para los clasificados de «secreto» o en armarios-archivadores metálicos y equipados con barras de cierre en acero, con candado cambiable, tipo combinación, o en otras instalaciones que garanticen unas condiciones de seguridad semejantes.

Artículo quince. *Cambio de combinaciones de cerraduras.*

Las combinaciones de las cerraduras de los equipos de seguridad sólo podrán ser cambiadas por personas que tengan el adecuado visado de seguridad y en los casos siguientes:

A) Que una persona conocedora de la combinación sea trasladada de la dependencia a que pertenece el equipo, o se la haya retirado el visado o credencial de seguridad.

B) Que la combinación haya sido sometida a reparación.

C) Siempre que el Jefe del Servicio de Protección de Materias Clasificadas lo estime oportuno, de acuerdo con el Ministro.

D) Como mínimo una vez al año.

Artículo dieciséis. *Marcas en documentos encuadernados, no encuadernados y en planos, croquis y otros documentos reservados.*

La clasificación asignada a documentos encuadernados, tales como libros o folletos cuyas páginas estén sólida y permanentemente unidas, deberá estar visiblemente marcada o estampillada en el exterior de la cubierta frontal, en la página del titulo, en la primera página, en la última página y en el exterior de la cubierta posterior. En cada caso, las marcas se estamparan en la parte superior e inferior de la página o cubierta.

Si se tratase de documentos no encuadernados, tales como escritos, cartas, memorandums, informes, telegramas y otros documentos similares, cuyas páginas no están unidas de manera sólida y permanente, las marcas o estampillas deberán hacerse en la parte superior e inferior de cada página, de forma que la señal quede claramente visible cuando las paginas estén grapadas o sujetas con clips.

En el caso de planos, mapas, croquis, bocetos y demás documentos similares, la marca de clasificación se estampara bajo la leyenda, cuerpo o título o escala, de tal forma que quede claramente reproducida en todas las copias que de los mismos se obtengan. Dicha clasificación deberá ser marcada también en la parte superior e inferior en cada caso.

Artículo diecisiete. *Sustitución de funciones.*

Cuando la persona a cuya custodia estuvieren confiadas materias clasificadas fuere sustituida en las funciones que ejerciera, se ausentare por un periodo superior a quince días, o por cualquier otro motivo, no pudiere continuar ejerciendo tal encargo, deberá proceder a hacer entrega de aquéllos a persona reglamentariamente designada para sustituirla, mediante la elaboración de un inventario que deberá estar conformado por el funcionario entrante y el saliente.

Esta formalidad deberá cumplimentarse antes de que la persona a sustituir haya cesado de forma reglamentaria en el cargo.

Artículo dieciocho. *Traslado del material «secreto».*

El traslado fuera de los lugares específicamente destinados a la custodia de material clasificado como «secreto» se llevará a cabo de la siguiente forma:

Se hará cubierta interior y exterior opacas. La cubierta interior será lacrada y con sello de seguridad, con la indicación de «secreto», la dirección a donde aquel se transmite y con la indicación de que sólo podrá ser abierta por su destinatario.

En la cubierta exterior, también debidamente lacrada, sólo figurará la dirección correspondiente, sin ningún índice de la clasificación de su contenido.

Adjunto a la cubierta interior llevará un impreso de recepción o «recibo» que identificará al remitente, destinatario y documento o material, sin contener ninguna indicación secreta y que deberá devolverse firmado y sellado por el receptor.

Artículo diecinueve. *Traslado del material «reservado».*

Si se tratase de material clasificado de «reservado», su traslado deberá llevarse a cabo también en dos cubiertas, de las cuales la exterior no llevará ninguna clasificación de seguridad. La interior, precintada y sellada, con la Indicación escueta de la clasificación y la dirección a donde aquél se transmite.

En este caso, sólo se requerirá un recibí si el expedidor lo juzga necesario.

Artículo veinte. *Transmisión del material «secreto».*

La transmisión de material secreto se llevará a cabo, preferiblemente, por medio de contacto directo de los funcionarios a quienes tal función corresponda, o por personal específicamente designado, valija diplomática, por un sistema de correos creado expresamente para este fin o por medios de transmisión en forma cifrada.

Artículo veintiuno. *Transmisión del material «reservado».*

La de material reservado se llevará a cabo de la misma manera que la expuesta para el secreto en el articulo anterior o por medio de los comandantes de aeronaves o navíos con categoría de oficial o correo certificado si no fuere practicable ninguno de los procedimientos anteriores, cifrándose los textos siempre que sea posible.

Artículo veintidós. *Transmisión dentro del órgano de origen.*

Si la transmisión de material clasificado se llevase a cabo dentro del órgano de origen, se regirá por las normas que elabore el Servicio de Protección de Materias Clasificadas correspondiente, las cuales deberán garantizar un grado de seguridad equivalente al indicado para transmisión fuera del mismo.

Artículo veintitrés. *Control de transmisión.*

En todo tiempo se mantendrá un control adecuado de la transmisión de material clasificado, llevándose un registro contable exacto del material transmitido, con una severa limitación del número de documentos entregados y copias que de los mismos se hagan.

Artículo veinticuatro. *Prohibición de la información por teléfono.*

La información clasificada no podrá ser transmitida o revelada por medio del teléfono, excepto en los casos en que así se disponga, expresamente, por medio de determinados circuitos, tanto civiles como militares.

Artículo veinticinco. *Registro de material clasificado.*

La persona responsable del Servicio de Protección de Materias Clasificadas supervisará el registro de todo el material clasificado en un Impreso especial, en el cual figurarán el órgano de origen, la fecha y la calificación correspondiente; el movimiento de tal material y

su destrucción, en su caso. Cada impreso especial deberá referirse a una materia, pudiéndose agrupar en un solo legajo todo el material que se refiera al mismo concepto.

Todos los ejemplares de un documento clasificado serán numerados por la Autoridad encargada de la calificación, y lo mismo deberá hacerse cuando una entidad distinta fuere autorizada para su reproducción. En este caso, la Autoridad encargada de calificar indicará los números correspondientes a los ejemplares de copia.

A continuación del número de ejemplares deberá figurar el número de folios del mismo.

Artículo veintiséis. *Inventario del material clasificado.*

En todos los Servicios de Protección de Materias Clasificadas, la persona responsable de los mismos procederá a realizar un inventario en el mes de enero de cada año. De su resultado se remitirá certificación al Ministro del Departamento, quien la devolverá con su conformidad o reparos.

Artículo veintisiete. *Examen del material clasificado.*

El examen de materias clasificadas sólo se autorizará mediante expedición de la correspondiente autorización por la Autoridad encargada de la calificación, a personas cuyos deberes oficiales requieren tal acceso, y con especificación de si se trata de una sola vez o con carácter habitual y ello, únicamente, si han sido calificadas en aquella autorización como personal de confianza.

En todo caso, en el Servicio de Protección de Materias Clasificadas se llevará un registro contable de las personas a las cuales se haya facilitado acceso al material clasificado, incorporándose un ejemplar, de un documento debidamente firmado por el Jefe del Servicio y la persona autorizada, al legajo correspondiente con especificación de las circunstancias personales, fecha. Autoridad que extendió la autorización y contenido de ésta.

Por otra parte, y a menos que en la autorización se disponga expresamente lo contrario, no se permitirá, en ningún caso, la toma de notas, datos y demás pormenores del material correspondiente.

La persona responsable del Servicio, por sí o por medio de otra persona a sus órdenes, y de cuya actuación sea aquélla responsable, deberá estar presente en todo momento, mientras dure el examen del material.

Artículo veintiocho. *Destrucción de material clasificado.*

Siempre que la Autoridad encargada de la calificación juzgare que el material clasificado resultare ya inservible, ordenará su destrucción a todas las dependencias que lo poseyeren o hubiesen obtenido copias o reproducciones del mismo.

Nadie podrá, en circunstancias normales, destruir material clasificado sin haber obtenido, previamente, autorización de aquella Autoridad.

Si algún Organismo, luego de haber recibido orden de destrucción de determinado material clasificado, entendiese que algún ejemplar continúa siendo necesario, solicitará, motivadamente, de la Autoridad calificadora, la correspondiente autorización para conservarlo.

Artículo veintinueve. *Procedimientos de destrucción y destrucción de emergencia del material clasificado.*

El material clasificado será destruido por medio del fuego, procedimientos químicos o, cuando tales medios no existan, por medio de artefactos que los reduzcan a pulpa o fragmentos tan minúsculos que imposibiliten su reconstrucción.

En todo caso, la destrucción habrá de ser completa.

Artículo treinta.

La destrucción deberá llevarse a cabo bajo la supervisión de la persona responsable del Servicio de Protección de Materias Clasificadas, debiendo ser certificada por el mismo y dándose cuenta inmediatamente de ello, por conducto reglamentario, a la autoridad calificadora.

Dichos certificados de destrucción serán numerados dentro de cada año por el Organismo interesado. En la hoja de control del Organismo que procedió a la distribución del material o autorizó su destrucción deberá cumplimentarse el espacio referente a la recepción de los certificados.

Artículo treinta y uno.

Todos los Organismos poseedores de material clasificado deberán tener previsto, para casos de emergencia, un plan de destrucción del conjunto de aquél.

Dicho plan deberá ser estudiado por la persona responsable del Servicio de Protección de Materias Clasificadas, la cual, a la vista de los sistemas más accesibles y adecuados, deberá adoptar las medidas necesarias para su inmediata y rápida ejecución.

Artículo treinta y dos.

Cualquier persona que tuviere a su cargo la elaboración o copia de material clasificable, deberá adoptar las medidas tendentes a que sean destruidos, en el más breve plazo posible, los borradores, minutas, hojas inutilizadas y papeles químicos u otros elementos que hayan servido para tales fines.

Artículo treinta y tres. *Programas de entrenamiento y ordenación.*

Las personas responsables de los Servicios de Protección de Materias Clasificadas establecerán y mantendrán programas activos de entrenamiento y orientación para loe funcionarios que en ellos presten sus servicios, a fin de inculcarles el sentido de la responsabilidad personal que, a cada uno, incumbe, en orden a proceder, en todo momento, con especial vigilancia y cuidado, al cumplimiento de las órdenes que reciba y a la más estricta observancia de las medidas de protección vigentes.

Como mínimo, dichos programas habrán de comprender:

A) Precisa explicación y análisis de las medidas de protección.

B) Formas de llevar a cabo su más exacto cumplimiento.

C) Identificación de personas y comprobación de autorizaciones de acceso a las materias clasificadas.

D) Las normas sobre utilización, conservación y destrucción cuando fueren pertinentes y oportunas.

E) Medidas correspondientes antes y durante el traslado o transmisión del material clasificado.

F) Cualesquiera otras que tiendan a la mejor consecución de los fines perseguidos.

Artículo treinta y cuatro. *Calificación de las faltas disciplinarias y administrativas.*

La difusión o publicación de las actividades reservadas por declaración de Ley, o de «materias clasificadas», tanto por parte del personal adscrito a los Servicios de Protección de Materias Clasificadas, cuanto por cualesquiera otras personas al servicio de la Administración, aparte la responsabilidad penal que, en su caso, produjeren, tendrán la consideración, a efectos disciplinarios y administrativos, de faltas muy graves.

En las restantes violaciones de las normas contenidas en este Decreto, la gravedad de la falta será determinada por la naturaleza de la infracción y por las posibles consecuencias que de ella pudieran derivarse.

Artículo treinta y cinco.

De conformidad con lo dispuesto en el artículo catorce de la Ley, la calificación de secreto o reservado no impedirá el exacto cumplimiento de los trámites de audiencia, alegaciones, notificaciones directas a los Interesados, en la forma establecida en la Ley de Procedimiento Administrativo, sin perjuicio de la eventual aplicación de las sanciones previstas en caso de violación del secreto por parte de los interesados.

Disposición adicional.

De acuerdo con lo establecido en los artículos nueve, apartado C), y once, apartado E), del presente Decreto, y teniendo en cuenta las especiales características de todo orden que concurren en el normal desenvolvimiento de la función que a las Fuerzas Armadas atribuye la Ley Orgánica del Estado, los Departamentos ministeriales correspondientes, sin perjuicio de lo dispuesto con carácter general en este Decreto, podrán elaborar normas específicas de régimen Interior para el mejor cumplimiento de la alta misión que, por precepto legal, les está encomendada.

De la misma manera y en atención a las peculiares características del servicio diplomático y a las circunstancias en que éste desarrolla sus funciones fuera del territorio nacional, el Ministerio de Asuntos Exteriores podrá elaborar también normas específicas de régimen interior para sus oficinas en el extranjero, sin perjuicio de las normas de carácter general contenidas en el presente Decreto.

§ 17

Ley Orgánica 4/1981, de 1 de junio, de los estados de alarma, excepción y sitio

Jefatura del Estado
«BOE» núm. 134, de 5 de junio de 1981
Última modificación: sin modificaciones
Referencia: BOE-A-1981-12774

DON JUAN CARLOS I, REY DE ESPAÑA

A todos los que la presente vieren y entendieren,

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente Ley Orgánica:

CAPÍTULO PRIMERO

Disposiciones comunes a los tres estados

Artículo primero.

Uno. Procederá la declaración de los estados de alarma, excepción o sitio cuando circunstancias extraordinarias hiciesen imposible el mantenimiento de la normalidad mediante los poderes ordinarios de las Autoridades competentes.

Dos. Las medidas a adoptar en los estados de alarma, excepción y sitio, así como la duración de los mismos, serán en cualquier caso las estrictamente indispensables para asegurar el restablecimiento de la normalidad. Su aplicación se realizará de forma proporcionada a las circunstancias.

Tres. Finalizada la vigencia de los estados de alarma, excepción y sitio decaerán en su eficacia cuantas competencias en materia sancionadora y en orden a actuaciones preventivas correspondan a las Autoridades competentes, así como las concretas medidas adoptadas en base a éstas, salvo las que consistiesen en sanciones firmes.

Cuatro. La declaración de los estados de alarma, excepción y sitio no interrumpe el normal funcionamiento de los poderes constitucionales del Estado.

Artículo segundo.

La declaración de los estados de alarma, excepción o sitio será publicada de inmediato en el «Boletín Oficial del Estado», y difundida obligatoriamente por todos los medios de comunicación públicos y por los privados que se determinen, y entrará en vigor desde el instante mismo de su publicación en aquél. También serán de difusión obligatoria las disposiciones que la Autoridad competente dicte durante la vigencia de cada uno de dichos estados.

Artículo tercero.

Uno. Los actos y disposiciones de la Administración Pública adoptados durante la vigencia de los estados de alarma, excepción y sitio serán impugnables en vía jurisdiccional de conformidad con lo dispuesto en las leyes.

Dos. Quienes como consecuencia de la aplicación de los actos y disposiciones adoptadas durante la vigencia de estos estados sufran, de forma directa, o en su persona, derechos o bienes, daños o perjuicios por actos que no les sean imputables, tendrán derecho a ser indemnizados de acuerdo con lo dispuesto en las leyes.

CAPÍTULO II

El estado de alarma

Artículo cuarto.

El Gobierno, en uso de las facultades que le otorga el artículo ciento dieciséis, dos, de la Constitución podrá declarar el estado de alarma, en todo o parte del territorio nacional, cuando se produzca alguna de las siguientes alteraciones graves de la normalidad.

a) Catástrofes, calamidades o desgracias públicas, tales como terremotos, inundaciones, incendios urbanos y forestales o accidentes de gran magnitud.

b) Crisis sanitarias, tales como epidemias y situaciones de contaminación graves.

c) Paralización de servicios públicos esenciales para la comunidad, cuando no se garantice lo dispuesto en los artículos veintiocho, dos, y treinta y siete, dos, de la Constitución, concurra alguna de las demás circunstancia o situaciones contenidas en este artículo.

d) Situaciones de desabastecimiento de productos de primera necesidad.

Artículo quinto.

Cuando los supuestos a que se refiere el artículo anterior afecten exclusivamente a todo, o parte del ámbito territorial de una Comunidad Autónoma, el Presidente de la misma, podrá solicitar del Gobierno la declaración de estado de alarma.

Artículo sexto.

Uno. La declaración del estado de alarma se llevará a cabo mediante decreto acordado en Consejo de Ministros.

Dos. En el decreto se determinará el ámbito territorial, la duración y los efectos del estado de alarma, que no podrá exceder de quince días. Sólo se podrá prorrogar con autorización expresa del Congreso de los Diputados, que en este caso podrá establecer el alcance y las condiciones vigentes durante la prórroga.

Artículo séptimo.

A los efectos del estado de alarma la Autoridad competente será el Gobierno o, por delegación de éste, el Presidente de la Comunidad Autónoma cuando la declaración afecte exclusivamente a todo o parte del territorio de una Comunidad.

Artículo octavo.

Uno. El Gobierno dará cuenta al Congreso de los Diputados de la declaración del estado de alarma y le suministrará la información que le sea requerida.

Dos. El Gobierno también dará cuenta al Congreso de los Diputados de los decretos que dicte durante la vigencia del estado de alarma en relación con éste.

Artículo noveno.

Uno. Por la declaración del estado de alarma todas las Autoridades civiles de la Administración Pública del territorio afectado por la declaración, los integrantes de los Cuerpos de Policía de las Comunidades Autónomas y de las Corporaciones Locales, y los

demás funcionarios y trabajadores al servicio de las mismas, quedarán bajo las órdenes directas de la Autoridad competente en cuanto sea necesaria para la protección de personas, bienes y lugares, pudiendo imponerles servicios extraordinarios por su duración o por su naturaleza.

Dos. Cuando la Autoridad competente sea el Presidente de una Comunidad Autónoma podrá requerir la colaboración de los Cuerpos y Fuerzas de Seguridad del Estado, que actuarán bajo la dirección de sus mandos naturales.

Artículo diez.

Uno. El incumplimiento o la resistencia a las órdenes de la Autoridad competente en el estado de alarma será sancionado con arreglo a lo dispuesto en las leyes.

Dos. Si estos actos fuesen cometidos por funcionarios, las Autoridades podrán suspenderlos de inmediato en el ejercicio de sus cargos, pasando, en su caso, el tanto de culpa al juez, y se notificará al superior jerárquico, a los efectos del oportuno expediente disciplinario.

Tres. Si fuesen cometidos por Autoridades, las facultades de éstas que fuesen necesarias para el cumplimiento de las medidas acordadas en ejecución de la declaración de estado de alarma podrán ser asumidas por la Autoridad competente durante su vigencia.

Artículo once.

Con independencia de lo dispuesto en el artículo anterior, el decreto de declaración del estado de alarma, o los sucesivos que durante su vigencia se dicten, podrán acordar las medidas siguientes:

a) Limitar la circulación o permanencia de personas o vehículos en horas y lugares determinados, o condicionarlas al cumplimiento de ciertos requisitos.

b) Practicar requisas temporales de todo tipo de bienes e imponer prestaciones personales obligatorias.

c) Intervenir y ocupar transitoriamente industrias, fábricas, talleres, explotaciones o locales de cualquier naturaleza, con excepción de domicilios privados, dando cuenta de ello a los Ministerios interesados.

d) Limitar o racionar el uso de servicios o el consumo de artículos de primera necesidad.

e) Impartir las órdenes necesarias para asegurar el abastecimiento de los mercados y el funcionamiento de los servicios de los centros de producción afectados por el apartado d) del artículo cuarto.

Artículo doce.

Uno. En los supuestos previstos en los apartados a) y b) del artículo cuarto, la Autoridad competente podrá adoptar por sí, según los casos, además de las medidas previstas en los artículos anteriores, las establecidas en las normas para la lucha contra las enfermedades infecciosas, la protección del medio ambiente, en materia de aguas y sobre incendios forestales.

Dos. En los casos previstos en los apartados c) y d) del artículo cuarto el Gobierno podrá acordar la intervención de empresas o servicios, así como la movilización de su personal, con el fin de asegurar su funcionamiento. Será de aplicación al personal movilizado la normativa vigente sobre movilización que, en todo caso, será supletoria respecto de lo dispuesto en el presente artículo.

CAPÍTULO III

El estado de excepción

Artículo trece.

Uno. Cuando el libre ejercicio de los derechos y libertades de los ciudadanos, el normal funcionamiento de las instituciones democráticas, el de los servicios públicos esenciales para la comunidad, o cualquier otro aspecto del orden público, resulten tan gravemente

alterados que el ejercicio de las potestades ordinarias fuera insuficiente para restablecerlo y mantenerlo, el Gobierno, de acuerdo con el apartado tres del artículo ciento dieciséis de la Constitución, podrá solicitar del Congreso de los Diputados autorización para declarar el estado de excepción.

Dos. A los anteriores efectos, el Gobierno remitirá al Congreso de los Diputados una solicitud de autorización que deberá contener los siguientes extremos:

a) Determinación de los efectos del estado de excepción, con mención expresa de los derechos cuya suspensión se solicita, que no podrán ser otros que los enumerados en el apartado uno del artículo cincuenta y cinco de la Constitución.

b) Relación de las medidas a adoptar referidas a los derechos cuya suspensión específicamente se solicita.

c) Ámbito territorial del estado de excepción, así como duración del mismo, que no podrá exceder de treinta días.

d) La cuantía máxima de las sanciones pecuniarias que la Autoridad gubernativa esté autorizada para imponer, en su caso, a quienes contravengan las disposiciones que dicte durante el estado de excepción.

Tres. El Congreso debatirá la solicitud de autorización remitida por el Gobierno, pudiendo aprobarla en sus propios términos o introducir modificaciones en la misma.

Artículo catorce.

El Gobierno, obtenida la autorización a que hace referencia el artículo anterior, procederá a declarar el estado de excepción, acordando para ello en Consejo de Ministros un decreto con el contenido autorizado por el Congreso de los Diputados.

Artículo quince.

Uno. Si durante el estado de excepción, el Gobierno considerase conveniente la adopción de medidas distintas de las previstas en el decreto que lo declaró, procederá a solicitar del Congreso de los Diputados la autorización necesaria para la modificación del mismo, para lo que se utilizará el procedimiento, que se establece en los artículos anteriores.

Dos. El Gobierno, mediante decreto acordado en Consejo de Ministros, podrá poner fin al estado de excepción antes de que finalice el período para el que fue declarado, dando cuenta de ello inmediatamente al Congreso de los Diputados.

Tres. Si persistieran las circunstancias que dieron lugar a la declaración del estado de excepción, el Gobierno podrá solicitar del Congreso de los Diputados la prórroga de aquél, que no podrá exceder de treinta días.

Artículo dieciséis.

Uno. La Autoridad gubernativa podrá detener a cualquier persona si lo considera necesario para la conservación del orden, siempre que, cuando menos, existan fundadas sospechas de que dicha persona vaya a provocar alteraciones del orden público. La detención no podrá exceder de diez días y los detenidos disfrutarán de los derechos que les reconoce el artículo diecisiete, tres, de la Constitución.

Dos. La detención habrá de ser comunicada al juez competente en el plazo de veinticuatro horas. Durante la detención, el Juez podrá, en todo momento, requerir información y conocer personalmente, o mediante delegación en el Juez de Instrucción del partido o demarcación donde se encuentre el detenido la situación de éste.

Artículo diecisiete.

Uno. Cuando la autorización del Congreso comprenda la suspensión del artículo dieciocho, dos, de la Constitución, la Autoridad gubernativa podrá disponer inspecciones, registros domiciliarios si lo considera necesario para el esclarecimiento de los hechos presuntamente delictivos o para el mantenimiento del orden público.

Dos. La inspección o el registro se llevarán a cabo por la propia Autoridad o por sus agentes, a los que proveerá de orden formal y escrita.

Tres. El reconocimiento de la casa, papeles y efectos, podrá ser presenciado por el titular o encargado de la misma o por uno o más individuos de su familia mayores de edad y, en todo caso, por dos vecinos de la casa o de las inmediaciones, si en ellas los hubiere, o, en su defecto, por dos vecinos del mismo pueblo o del pueblo o pueblos limítrofes.

Cuatro. No hallándose en ella al titular o encargado de la casa ni a ningún individuo de la familia, se hará el reconocimiento en presencia únicamente de los dos vecinos indicados.

Cinco. La asistencia de los vecinos requeridos para presenciar el registro será obligatoria y coercitivamente exigible.

Seis. Se levantará acta de la inspección o registro, en la que se harán constar los nombres de las personas que asistieren y las circunstancias que concurriesen, así como las incidencias a que diere lugar. El acta será firmada por la autoridad o el agente que efectuare el reconocimiento y por el dueño o familiares y vecinos. Si no supieran o no quisiesen firmar se anotará también esta incidencia.

Siete. La autoridad gubernativa comunicará inmediatamente al Juez competente las inspecciones y registros efectuados, las causas que los motivaron y los resultados de los mismos, remitiéndole copia del acta levantada.

Artículo dieciocho.

Uno. Cuando la autorización del Congreso comprenda la suspensión del artículo dieciocho, tres, de la Constitución, la autoridad gubernativa podrá intervenir toda clase de comunicaciones, incluidas las postales, telegráficas y telefónicas. Dicha intervención sólo podrá ser realizada si ello resulta necesario para el esclarecimiento de los hechos presuntamente delictivos o el mantenimiento del orden público.

Dos. La intervención decretada será comunicada inmediatamente por escrito motivado al Juez competente.

Artículo diecinueve.

La autoridad gubernativa podrá intervenir y controlar toda clase de transportes, y la carga de los mismos.

Artículo veinte.

Uno. Cuando la autorización del Congreso comprenda la suspensión del artículo diecinueve de la Constitución, la autoridad gubernativa podrá prohibir la circulación de personas y vehículos en las horas y lugares que se determine, y exigir a quienes se desplacen de un lugar a otro que acrediten su identidad, señalándoles el itinerario a seguir.

Dos. Igualmente podrá delimitar zonas de protección o seguridad y dictar las condiciones de permanencia en las mismas y prohibir en lugares determinados la presencia de persona que puedan dificultar la acción de la fuerza pública.

Tres. Cuando ello resulte necesario, la Autoridad gubernativa podrá exigir a personas determinadas que comuniquen, con una antelación de dos días, todo desplazamiento fuera de la localidad en que tengan su residencia habitual.

Cuatro. Igualmente podrá disponer su desplazamiento fuera de dicha localidad cuando lo estime necesario.

Cinco. Podrá también fijar transitoriamente la residencia de personas determinadas en localidad o territorio adecuados a sus condiciones personales.

Seis. Corresponde a la Autoridad gubernativa proveer de los recursos necesarios para el cumplimiento de las medidas previstas en este artículo y, particularmente, de las referidas a viajes, alojamiento y manutención de la persona afectada.

Siete. Para acordar las medidas a que se refieren los apartados tres, cuatro y cinco de este artículo, la Autoridad gubernativa habrá de tener fundados motivos en razón a la peligrosidad que para el mantenimiento del orden público suponga la persona afectada por tales medidas.

Artículo veintiuno.

Uno. La Autoridad gubernativa podrá suspender todo tipo de publicaciones, emisiones de radio y televisión, proyecciones, cinematográficas y representaciones teatrales, siempre y

cuando la autorización del Congreso comprenda la suspensión del artículo veinte, apartados uno, a) y d), y cinco de la Constitución. Igualmente podrá ordenar el secuestro de publicaciones.

Dos. El ejercicio de las potestades a que se refiere el apartado anterior no podrá llevar aparejado ningún tipo de censura previa.

Artículo veintidós.

Uno. Cuando la autorización del Congreso comprenda la suspensión del artículo veintiuno de la Constitución, la autoridad gubernativa podrá someter a autorización previa o prohibir la celebración de reuniones y manifestaciones.

Dos. También podrá disolver las reuniones y manifestaciones a que se refiere el párrafo anterior.

Tres. Las reuniones orgánicas que los partidos políticos, los sindicatos y las asociaciones empresariales realicen en cumplimiento de los fines que respectivamente les asignen los artículos sexto y séptimo de la Constitución, y de acuerdo con sus Estatutos, no podrán ser prohibidas, disueltas ni sometidas a autorización previa.

Cuatro. Para penetrar en los locales en que tuvieran lugar las reuniones, la Autoridad gubernativa deberá proveer a sus agentes de autorización formal y escrita. Esta autorización no será necesaria cuando desde dichos locales se estuviesen produciendo alteraciones graves del orden público constitutivas del delito o agresiones a las Fuerzas de Seguridad y en cualesquiera otros casos de flagrante delito.

Artículo veintitrés.

La Autoridad gubernativa podrá prohibir las huelgas y la adopción de medidas de conflicto colectivo, cuando la autorización del Congreso comprenda la suspensión de los artículos veintiocho, dos, y treinta y siete, dos de la Constitución.

Artículo veinticuatro.

Uno. Los extranjeros que se encuentren en España vendrán obligados a realizar las comparecencias que se acuerden, a cumplir las normas que se dicten sobre renovación o control de permisos de residencia y cédulas de inscripción consular y a observar las demás formalidades que se establezcan.

Dos. Quienes contravinieren las normas o medidas que se adopten, o actuaren en connivencia con los perturbadores del orden público, podrán ser expulsados de España, salvo que sus actos presentaren indicios de ser constitutivos de delito, en cuyo caso se les someterá a los procedimientos judiciales correspondientes.

Tres. Los apátridas y refugiados respecto de los cuales no sea posible la expulsión se someterán al mismo régimen que los españoles.

Cuatro. Las medidas de expulsión deberán ir acompañadas de una previa justificación sumaria de las razones que la motivan.

Artículo veinticinco.

La autoridad gubernativa podrá proceder a la incautación de toda clase de armas, municiones o sustancias explosivas.

Artículo veintiséis.

Uno. La Autoridad gubernativa podrá ordenar la intervención de industrias o comercios que puedan motivar la alteración del orden público o coadyuvar a ella, y la suspensión temporal de las actividades de los mismos, dando cuenta a los Ministerios interesados.

Dos. Podrá, asimismo, ordenar el cierre provisional de salas de espectáculos, establecimientos de bebidas y locales de similares características.

Artículo veintisiete.

La Autoridad gubernativa podrá ordenar las medidas necesarias de vigilancia y protección de edificaciones, instalaciones, obras, servicios públicos e industrias o

explotaciones de cualquier género. A estos efectos podrá emplazar puestos armados en los lugares más apropiados para asegurar la vigilancia, sin perjuicio de lo establecido en el artículo dieciocho, uno de la Constitución.

Artículo veintiocho.

Cuando la alteración del orden público haya dado lugar a alguna de las circunstancias especificadas en el artículo cuarto coincida con ellas, el Gobierno podrá adoptar además de las medidas propias del estado de excepción, las previstas para el estado de alarma en la presente ley.

Artículo veintinueve.

Si algún funcionario o personal al servicio de una Administración pública o entidad o instituto de carácter público u oficial favoreciese con su conducta la actuación de los elementos perturbadores del orden, la Autoridad gubernativa podrá suspenderlo en el ejercicio de su cargo, pasando el tanto de culpa al Juez competente y notificándolo al superior jerárquico a los efectos del oportuno expediente disciplinario.

Artículo treinta.

Uno. Si durante el estado de excepción el Juez estimase la existencia de hechos contrarios al orden público o a la seguridad ciudadana que puedan ser constitutivos de delito, oído el Ministerio Fiscal, decretará la prisión provisional del presunto responsable, la cual mantendrá, según su arbitrio, durante dicho estado.

Dos. Los condenados en estos procedimientos quedan exceptuados de los beneficios de la remisión condicional durante la vigencia del estado de excepción.

Artículo treinta y uno.

Cuando la declaración del estado de excepción afecte exclusivamente a todo o parte del ámbito territorial de una Comunidad Autónoma, la Autoridad gubernativa podrá coordinar el ejercicio de sus competencias con el Gobierno de dicha Comunidad.

CAPÍTULO IV

El estado de sitio

Artículo treinta y dos.

Uno. Cuando se produzca o amenace producirse una insurrección o acto de fuerza contra la soberanía o independencia de España, su integridad territorial o el ordenamiento constitucional, que no pueda resolverse por otros medios, el Gobierno, de conformidad con lo dispuesto en el apartado cuatro del artículo ciento dieciséis de la Constitución, podrá proponer al Congreso de los Diputados la declaración de estado de sitio.

Dos. La correspondiente declaración determinará el ámbito territorial, duración y condiciones del estado de sitio.

Tres. La declaración podrá autorizar, además de lo previsto para los estados de alarma y excepción, la suspensión temporal de las garantías jurídicas del detenido que se reconocen en el apartado tres del artículo diecisiete de la Constitución.

Artículo treinta y tres.

Uno. En virtud de la declaración del estado de sitio, el Gobierno, que dirige la política militar y de la defensa, de acuerdo con el artículo noventa y siete de la Constitución, asumirá todas las facultades extraordinarias previstas en la misma y en la presente ley.

Dos. A efectos de lo dispuesto en el párrafo anterior, el Gobierno designará la Autoridad militar que, bajo su dirección, haya de ejecutar las medidas que procedan en el territorio a que el estado de sitio se refiera.

Artículo treinta y cuatro.

La Autoridad militar procederá a publicar y difundir los oportunos bandos, que contendrán las medidas y prevenciones necesarias, de acuerdo con la Constitución, la presente ley y las condiciones de la declaración del estado de sitio.

Artículo treinta y cinco.

En la declaración del estado de sitio el Congreso de los Diputados podrá determinar los delitos que durante su vigencia quedan sometidos a la Jurisdicción Militar.

Artículo treinta y seis.

Las Autoridades civiles continuarán en el ejercicio de las facultades que no hayan sido conferidas a la Autoridad militar de acuerdo con la presente Ley. Aquellas Autoridades darán a la militar las informaciones que ésta le solicite y cuantas noticias referentes al orden público lleguen a su conocimiento.

DISPOSICIÓN DEROGATORIA

Quedan derogados los artículos veinticinco a cincuenta y uno y disposiciones finales y transitorias de la Ley cuarenta y cinco mil novecientos cincuenta y nueve, de treinta de julio, de Orden Público, así como cuantas disposiciones se opongan a lo preceptuado en la presente Ley Orgánica.

DISPOSICIÓN FINAL

La presente Ley entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

§ 18

Ley 1/2019, de 20 de febrero, de Secretos Empresariales

Jefatura del Estado
«BOE» núm. 45, de 21 de febrero de 2019
Última modificación: sin modificaciones
Referencia: BOE-A-2019-2364

FELIPE VI

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley:

PREÁMBULO

I

La innovación es un importante estímulo para el desarrollo de nuevos conocimientos y propicia la emergencia de modelos empresariales basados en la utilización de conocimientos adquiridos colectivamente. Las organizaciones valoran sus secretos empresariales tanto como los derechos de propiedad industrial e intelectual y utilizan la confidencialidad como una herramienta de gestión de la competitividad empresarial, de transferencia de conocimiento público-privada y de la innovación en investigación, con el objetivo de proteger información que abarca no solo conocimientos técnicos o científicos, sino también datos empresariales relativos a clientes y proveedores, planes comerciales y estudios o estrategias de mercado.

Sin embargo, las entidades innovadoras están cada vez más expuestas a prácticas desleales que persiguen la apropiación indebida de secretos empresariales, como el robo, la copia no autorizada, el espionaje económico o el incumplimiento de los requisitos de confidencialidad. La globalización, una creciente externalización, cadenas de suministro más largas y un mayor uso de las tecnologías de la información y la comunicación, contribuyen a aumentar el riesgo de tales prácticas.

La obtención, utilización o revelación ilícitas de un secreto empresarial comprometen la capacidad de su titular legítimo para aprovechar las ventajas que le corresponden como precursor por su labor de innovación. La falta de instrumentos jurídicos eficaces y comparables para la protección de los secretos empresariales menoscaba los incentivos para emprender actividades asociadas a la innovación e impiden que los secretos empresariales puedan liberar su potencial como estímulos del crecimiento económico y del empleo. En consecuencia, la innovación y la creatividad se ven desincentivadas y disminuye

la inversión, con las consiguientes repercusiones en el buen funcionamiento del mercado y la consiguiente merma de su potencial como factor de crecimiento.

Es necesario garantizar que la competitividad, que se sustenta en el saber hacer y en información empresarial no divulgada, esté protegida de manera adecuada, y mejorar las condiciones y el marco para el desarrollo y la explotación de la innovación y la transferencia de conocimientos en el mercado.

Una seguridad jurídica reforzada contribuiría a aumentar el valor de las innovaciones que las organizaciones tratan de proteger como secretos empresariales, ya que se reduciría el riesgo de apropiación indebida. Esto redundaría en efectos positivos en el funcionamiento del mercado, ya que las empresas, especialmente las pequeñas y medianas empresas, los centros públicos de investigación y los investigadores podrían hacer un mejor uso de sus ideas innovadoras, cooperando, lo que contribuiría a aumentar la inversión del sector privado en investigación e innovación.

II

Los esfuerzos emprendidos a nivel internacional en el marco de la Organización Mundial del Comercio para poner remedio a este problema tuvieron reflejo en el Acuerdo sobre los Aspectos de los Derechos de Propiedad intelectual relacionados con el Comercio (Anexo 1C del Convenio por el que se crea la Organización Mundial del Comercio, Ronda Uruguay de 1994, comúnmente denominados «ADPIC»). Este acuerdo contiene, entre otras, unas disposiciones relativas a la protección de los secretos empresariales contra su obtención, utilización o revelación ilícitas por terceros, que constituyen normas internacionales comunes. Todos los Estados miembros de la Unión Europea, así como la propia Unión, están vinculados por dicho acuerdo, que fue aprobado mediante la Decisión 94/800/CE del Consejo, de 22 de diciembre de 1994, relativa a la celebración en nombre de la Comunidad Europea, por lo que respecta a los temas de su competencia, de los acuerdos resultantes de las negociaciones multilaterales de la Ronda Uruguay (1986-1994).

En este contexto, dentro de la Unión Europea las divergencias nacionales existentes en materia de protección de secretos empresariales han llevado a la aprobación de la Directiva (UE) 2016/943 del Parlamento Europeo y del Consejo, de 8 de junio de 2016, relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas, a fin de armonizar la legislación de los Estados miembros con el objetivo de establecer un nivel suficiente y comparable de reparación en todo el mercado interior en caso de apropiación indebida de secretos empresariales.

El objetivo de la iniciativa europea es, por un lado, garantizar que la competitividad de las empresas y organismos de investigación europeos que se basa en el saber hacer y en información empresarial no divulgada (secretos empresariales) esté protegida de manera adecuada y, por otro, mejorar las condiciones y el marco para el desarrollo y la explotación de la innovación y la transferencia de conocimientos en el mercado interior.

La directiva contiene normas en materia de protección frente a la obtención, utilización y revelación ilícitas de secretos empresariales que no podrán invocarse para restringir la libertad de establecimiento, la libre circulación de los trabajadores o la movilidad de éstos y que tampoco afectan a la posibilidad de que los empresarios y los trabajadores celebren pactos de limitación de la competencia entre ellos.

Se define el objeto de esta norma como aquella información que sea secreta en el sentido de no ser, en su conjunto o en la configuración y reunión precisas de sus componentes, generalmente conocida por las personas pertenecientes a los círculos en que normalmente se utilice el tipo de información en cuestión, ni fácilmente accesible para estas; tenga un valor comercial por su carácter secreto, y haya sido objeto de medidas razonables, en las circunstancias del caso, para mantenerla secreta, tomadas por la persona que legítimamente ejerza su control. Por consiguiente, esta definición de secreto empresarial no abarca la información de escasa importancia, como tampoco la experiencia y las competencias adquiridas por los trabajadores durante el normal transcurso de su carrera profesional ni la información que es de conocimiento general o fácilmente accesible en los círculos en que normalmente se utilice el tipo de información en cuestión.

Se establecen asimismo las circunstancias en las que está justificada su protección jurídica, así como los comportamientos y prácticas que son constitutivos de obtención, utilización o revelación ilícita del mismo.

Las vías de acción civil frente a la obtención, utilización o revelación ilícitas de secretos empresariales no deben comprometer ni menoscabar los derechos y libertades fundamentales ni el interés público y han de ser aplicadas de forma proporcionada, evitando la creación de obstáculos al comercio legítimo en el mercado interior y previendo medidas de salvaguarda contra los abusos.

En este nuevo marco jurídico, la presente ley, que, con arreglo al artículo 25 de la Ley 50/1997, de 27 de noviembre, del Gobierno, está incluida en el Plan Anual Normativo de 2018, aborda el mandato de transposición de la citada directiva y, con el fin de incorporarla a nuestro ordenamiento jurídico, busca mejorar la eficacia de la protección jurídica de los secretos empresariales contra la apropiación indebida en todo el mercado interior completando la regulación de la Ley 3/1991, de 10 de enero, de Competencia Desleal, y en concreto su artículo 13, desde una perspectiva sustantiva y, especialmente, procesal.

Los criterios seguidos en la transposición se han basado en los principios de la buena regulación, comprendiendo el principio de necesidad y eficacia al cumplir la obligación de transposición con fidelidad al texto de la directiva y con la mínima reforma de la actual normativa, de manera que se evite la dispersión en aras de la simplificación; así como en los principios de proporcionalidad, al contener la regulación imprescindible para atender la necesidad a cubrir, y de seguridad jurídica, ya que se realiza con el ánimo de mantener un marco normativo estable, predecible, integrado y claro.

III

La ley se estructura en veinticinco artículos distribuidos en cinco capítulos, una disposición transitoria y seis disposiciones finales.

El Capítulo I se inicia con la descripción del objeto de la ley, esto es, la protección de los secretos empresariales, estableciendo su definición conforme a los dictados de la Directiva (UE) 2016/943 del Parlamento Europeo y del Consejo, de 8 de junio de 2016. Esta definición constituye una de las novedades más sobresalientes de la presente ley, que configura dicha noción abarcando cualquier información que sea secreta, tenga valor empresarial y haya sido objeto de medidas razonables por parte de su titular para mantenerla en secreto.

Se ha considerado igualmente conveniente en todo caso preservar la terminología tradicionalmente empleada en nuestro sistema jurídico en los casos en los que los nuevos términos se refieren a conceptos sobradamente arraigados, estudiados y tratados en la legislación, la jurisprudencia y la doctrina. En este sentido, por ejemplo, se ha preferido mantener las expresiones de «secretos empresariales» para designar el objeto de protección y de «titular» para designar a quien legítimamente posee el secreto empresarial y se beneficia de su protección jurídica. Las disposiciones de esta ley atribuyen al titular del secreto empresarial un derecho subjetivo de naturaleza patrimonial, susceptible de ser objeto de transmisión, en particular, de cesión o transmisión a título definitivo y de licencia o autorización de explotación con el alcance objetivo, material, territorial y temporal que en cada caso se pacte.

El Capítulo II define, por un lado, las circunstancias en las que la obtención, utilización y revelación de secretos empresariales son consideradas lícitas en consideración a intereses dignos de una mayor tutela y por tanto, frente a las que no procederán las medidas de protección previstas en esta ley; y, por otro, las conductas constitutivas de violación de secretos empresariales. En este sentido, la protección de los secretos empresariales se extiende también de forma novedosa a las llamadas «mercancías infractoras» incluyéndose los actos de explotación de estas mercancías entre los que constituyen violación de secreto empresarial.

El Capítulo III, sin tener origen directo en el articulado de la directiva, complementa y perfecciona su contenido, al abordar, mediante reglas dispositivas, la vertiente patrimonial del secreto empresarial. Se trata, en definitiva, de previsiones que, en defecto de acuerdo entre las partes, ordenan someramente cómo se desenvuelve la potencial cotitularidad del secreto empresarial y su transmisibilidad, en particular si se acomete mediante licencia contractual.

Por su parte, en el Capítulo IV se consigna un catálogo abierto de acciones de defensa que contiene la designación y configuración sustantiva de los más importantes remedios reconocidos al titular del secreto empresarial para hacer frente a su violación, con especial atención a la regulación de la indemnización de daños y perjuicios, que se extiende tanto a su contenido económico como a la facilitación de su cálculo y liquidación en línea con lo ya dispuesto en materia de infracción de patentes y por extensión de otros derechos de propiedad industrial. Por último, la regulación material de las acciones de defensa concluye con una regla propia de prescripción.

Finalmente, el Capítulo V viene a regular aquellos aspectos procesales que permiten ofrecer a los titulares de secretos empresariales herramientas efectivas para la tutela judicial de su posición jurídica, a través de un sistema de acciones robusto y de un proceso plenamente eficaz y sencillo, respetuoso con las garantías de justicia y equidad pero desprovisto de formalidades innecesarias y concebido para tramitarse en un plazo razonable, cuya eficacia se asegura en todo caso a través de un catálogo adecuado de medidas cautelares. Las acciones de defensa de los secretos empresariales habrán de aplicarse de forma proporcionada y evitando tanto la creación de obstáculos al libre comercio como su ejercicio de forma abusiva o de mala fe. A este respecto, se agravan las medidas que los jueces y tribunales pueden adoptar con carácter general por incumplimiento de las reglas de la buena fe procesal, para impedir que, bajo la cobertura de la supuesta defensa de un secreto empresarial, se utilicen las acciones previstas en esta ley con la finalidad de ejercer una indebida presión sobre quien ha obtenido algún tipo de información cuya divulgación pudiera estar cubierta por alguna de las excepciones que contempla la directiva y aquí se transponen.

Por lo demás, las novedades procesales más significativas se proyectan sobre tres aspectos. En primer lugar, se incorporan una serie de reglas al objeto de preservar el tratamiento confidencial de la información que se aporte o se genere en el proceso y que pueda constituir secreto empresarial. En segundo lugar, se ofrece un marco normativo para el desarrollo de diligencias de comprobación de hechos, de acceso a fuentes de prueba en poder de la contraparte o de terceros y, en su caso, de aseguramiento de pruebas. En tercer lugar, se incorporan reglas singulares en materia de tutela cautelar, así como especialidades en relación con la caución sustitutoria, el alzamiento de las medidas en caso de que durante la pendencia del litigio se produzca una desaparición sobrevenida del secreto empresarial y para la tutela de la posición jurídica de los terceros que se puedan ver o se hayan visto afectados desfavorablemente por las medidas cautelares.

En la parte final destaca la modificación del artículo 13 de la Ley 3/1991, de 10 de enero, de Competencia Desleal, para, manteniendo la atribución del carácter de competencia desleal a la violación de secretos empresariales, precisar que ésta se regirá por lo dispuesto en la presente norma, que actuará como ley especial frente a la previsiones de aquella disposición, susceptible, como ley general y en cuanto no se oponga a la especial, de ser utilizada para la integración de lagunas. De esta forma se perfila el encaje de la nueva ley dentro del marco de protección que nuestro ordenamiento jurídico proporciona frente a la violación de los secretos empresariales, sin perjuicio de las consecuencias que, para los casos más graves, resulta de la aplicación de los tipos delictivos contemplados en los artículos 278 y 279 del Código Penal.

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

1. El objeto de la presente ley es la protección de los secretos empresariales.

A efectos de esta ley, se considera secreto empresarial cualquier información o conocimiento, incluido el tecnológico, científico, industrial, comercial, organizativo o financiero, que reúna las siguientes condiciones:

a) Ser secreto, en el sentido de que, en su conjunto o en la configuración y reunión precisas de sus componentes, no es generalmente conocido por las personas

pertenecientes a los círculos en que normalmente se utilice el tipo de información o conocimiento en cuestión, ni fácilmente accesible para ellas;

b) tener un valor empresarial, ya sea real o potencial, precisamente por ser secreto, y

c) haber sido objeto de medidas razonables por parte de su titular para mantenerlo en secreto.

2. La protección se dispensa al titular de un secreto empresarial, que es cualquier persona física o jurídica que legítimamente ejerza el control sobre el mismo, y se extiende frente a cualquier modalidad de obtención, utilización o revelación de la información constitutiva de aquél que resulte ilícita o tenga un origen ilícito con arreglo a lo previsto en esta ley.

3. La protección de los secretos empresariales no afectará a la autonomía de los interlocutores sociales o a su derecho a la negociación colectiva. Tampoco podrá restringir la movilidad de los trabajadores; en particular, no podrá servir de base para justificar limitaciones del uso por parte de estos de experiencia y competencias adquiridas honestamente durante el normal transcurso de su carrera profesional o de información que no reúna todos los requisitos del secreto empresarial, ni para imponer en los contratos de trabajo restricciones no previstas legalmente.

Asimismo, lo dispuesto en esta ley se entenderá sin perjuicio de lo previsto en el Título IV de la Ley 24/2015, de 24 de julio, de Patentes.

CAPÍTULO II

Obtención, utilización y revelación de secretos empresariales

Artículo 2. *Obtención, utilización y revelación lícitas de secretos empresariales.*

1. La obtención de la información constitutiva del secreto empresarial se considera lícita cuando se realice por alguno de los medios siguientes:

a) El descubrimiento o la creación independientes;

b) La observación, estudio, desmontaje o ensayo de un producto u objeto que se haya puesto a disposición del público o esté lícitamente en posesión de quien realiza estas actuaciones, sin estar sujeto a ninguna obligación que válidamente le impida obtener de este modo la información constitutiva del secreto empresarial;

c) El ejercicio del derecho de los trabajadores y los representantes de los trabajadores a ser informados y consultados, de conformidad con el Derecho europeo o español y las prácticas vigentes;

d) Cualquier otra actuación que, según las circunstancias del caso, resulte conforme con las prácticas comerciales leales, incluidas la transferencia o cesión y la licencia contractual del secreto empresarial, de acuerdo con el Capítulo III.

2. La obtención, utilización o revelación de un secreto empresarial se consideran lícitas en los casos y términos en los que el Derecho europeo o español lo exija o permita.

3. En todo caso, no procederán las acciones y medidas previstas en esta ley cuando se dirijan contra actos de obtención, utilización o revelación de un secreto empresarial que hayan tenido lugar en cualquiera las circunstancias siguientes:

a) En ejercicio del derecho a la libertad de expresión e información recogido en la Carta de los Derechos Fundamentales de la Unión Europea, incluido el respeto a la libertad y al pluralismo de los medios de comunicación;

b) Con la finalidad de descubrir, en defensa del interés general, alguna falta, irregularidad o actividad ilegal que guarden relación directa con dicho secreto empresarial;

c) Cuando los trabajadores lo hayan puesto en conocimiento de sus representantes, en el marco del ejercicio legítimo por parte de estos de las funciones que tienen legalmente atribuidas por el Derecho europeo o español, siempre que tal revelación fuera necesaria para ese ejercicio;

d) Con el fin de proteger un interés legítimo reconocido por el Derecho europeo o español. En particular, no podrá invocarse la protección dispensada por esta ley para obstaculizar la aplicación de la normativa que exija a los titulares de secretos empresariales

divulgar información o comunicarla a las autoridades administrativas o judiciales en el ejercicio de las funciones de éstas, ni para impedir la aplicación de la normativa que prevea la revelación por las autoridades públicas europeas o españolas, en virtud de las obligaciones o prerrogativas que les hayan sido conferidas por el Derecho europeo o español, de la información presentada por las empresas que obre en poder de dichas autoridades.

Artículo 3. *Violación de secretos empresariales.*

1. La obtención de secretos empresariales sin consentimiento de su titular se considera ilícita cuando se lleve a cabo mediante:

a) El acceso, apropiación o copia no autorizadas de documentos, objetos, materiales, sustancias, ficheros electrónicos u otros soportes, que contengan el secreto empresarial o a partir de los cuales se pueda deducir; y

b) Cualquier otra actuación que, en las circunstancias del caso, se considere contraria a las prácticas comerciales leales.

2. La utilización o revelación de un secreto empresarial se consideran ilícitas cuando, sin el consentimiento de su titular, las realice quien haya obtenido el secreto empresarial de forma ilícita, quien haya incumplido un acuerdo de confidencialidad o cualquier otra obligación de no revelar el secreto empresarial, o quien haya incumplido una obligación contractual o de cualquier otra índole que limite la utilización del secreto empresarial.

3. La obtención, utilización o revelación de un secreto empresarial se consideran asimismo ilícitas cuando la persona que las realice, en el momento de hacerlo, sepa o, en las circunstancias del caso, debiera haber sabido que obtenía el secreto empresarial directa o indirectamente de quien lo utilizaba o revelaba de forma ilícita según lo dispuesto en el apartado anterior.

4. La producción, oferta o comercialización de mercancías infractoras o su importación, exportación o almacenamiento con tales fines constituyen utilizaciones ilícitas de un secreto empresarial cuando la persona que las realice sepa o, en las circunstancias del caso, debiera haber sabido que el secreto empresarial que incorporan se había utilizado de forma ilícita en el sentido de lo dispuesto en el apartado 2.

A efectos de la presente ley, se consideran mercancías infractoras aquellos productos y servicios cuyo diseño, características, funcionamiento, proceso de producción, o comercialización se benefician de manera significativa de secretos empresariales obtenidos, utilizados o revelados de forma ilícita.

CAPÍTULO III

El secreto empresarial como objeto del derecho de propiedad

Artículo 4. *Transmisibilidad del secreto empresarial.*

El secreto empresarial es transmisible.

En la transmisión habrán de observarse, cuando resulten aplicables por la naturaleza del secreto empresarial, los reglamentos de la Unión Europea relativos a la aplicación del apartado 3 del artículo 101 del Tratado de Funcionamiento de la Unión Europea a determinadas categorías de acuerdos de transferencia de tecnología.

Artículo 5. *Cotitularidad.*

1. El secreto empresarial podrá pertenecer pro indiviso a varias personas. La comunidad resultante se regirá por lo acordado entre las partes, en su defecto por lo dispuesto en los apartados siguientes y, en último término, por las normas de derecho común sobre la comunidad de bienes.

2. Cada uno de los partícipes por sí solo podrá:

a) Explotar el secreto empresarial previa notificación a los demás cotitulares.

b) Realizar los actos necesarios para la conservación del secreto empresarial como tal.

c) Ejercitar las acciones civiles y criminales en defensa del secreto empresarial, pero deberá notificarlo a los demás comuneros, a fin de que éstos puedan sumarse a las mismas, contribuyendo en tal supuesto al pago de los gastos habidos. En todo caso, si la acción resultase útil a la comunidad, todos los partícipes deberán contribuir al pago de dichos gastos.

3. La cesión del secreto empresarial o la concesión de licencia a un tercero para explotarlo deberá ser otorgada conjuntamente por todos los partícipes, a no ser que el órgano jurisdiccional por razones de equidad, dadas las circunstancias del caso, faculte a alguno de ellos para realizar la cesión o concesión mencionadas.

Artículo 6. *Licencias de secretos empresariales.*

1. El secreto empresarial puede ser objeto de licencia con el alcance objetivo, material, territorial y temporal que en cada caso se pacte. Salvo pacto en contrario, el titular de una licencia contractual tendrá derecho a realizar todos los actos que integran la utilización del secreto empresarial.

2. La licencia puede ser exclusiva o no exclusiva. Se presumirá que la licencia es no exclusiva y que el licenciante puede otorgar otras licencias o utilizar por sí mismo el secreto empresarial. La licencia exclusiva impide el otorgamiento de otras licencias y el licenciante sólo podrá utilizar el secreto empresarial si en el contrato se hubiera reservado expresamente ese derecho.

3. El titular de una licencia contractual no podrá cederla a terceros, ni conceder sublicencias, a no ser que se hubiere convenido lo contrario.

4. El licenciatario o sublicenciatario estará obligado a adoptar las medidas necesarias para evitar la violación del secreto empresarial.

Artículo 7. *Transmisión o licencia sin titularidad o facultades.*

Quien transmita a título oneroso un secreto empresarial u otorgue una licencia sobre el mismo responderá, salvo pacto en contrario, frente al adquirente de los daños que le cause, si posteriormente se declarara que carecía de la titularidad o de las facultades necesarias para la realización del negocio de que se trate. Responderá siempre cuando hubiera actuado de mala fe.

CAPÍTULO IV

Acciones de defensa de los secretos empresariales

Artículo 8. *Defensa de los secretos empresariales.*

Contra los infractores de un secreto empresarial podrán ejercitarse las acciones que correspondan, cualquiera que sea su clase y naturaleza, y exigir la adopción de las medidas necesarias para su protección.

A los efectos de esta norma se considerará infractor a toda persona física o jurídica que realice cualquier acto de violación de los enunciados en el artículo 3.

Asimismo, con las particularidades previstas en el artículo 9.7, dichas acciones podrán dirigirse frente a los terceros adquirentes de buena fe, entendiéndose por tales, a los efectos de la presente ley, quienes en el momento de la utilización o de la revelación no sabían o, en las circunstancias del caso, no hubieran debido saber que habían obtenido el secreto empresarial directa o indirectamente de un infractor.

Artículo 9. *Acciones civiles.*

1. Contra los actos de violación de secretos empresariales podrán, en especial, solicitarse:

a) La declaración de la violación del secreto empresarial.

b) La cesación o, en su caso, la prohibición de los actos de violación del secreto empresarial.

c) La prohibición de fabricar, ofrecer, comercializar o utilizar mercancías infractoras o de su importación, exportación o almacenamiento con dichos fines.

d) La aprehensión de las mercancías infractoras, incluida la recuperación de las que se encuentren en el mercado, y de los medios destinados únicamente a su producción, siempre que tal recuperación no menoscabe la protección del secreto comercial en cuestión, con una de las siguientes finalidades: su modificación para eliminar las características que determinen que las mercancías sean infractoras, o que los medios estén destinados únicamente a su producción, su destrucción o su entrega a entidades benéficas.

e) La remoción, que comprende la entrega al demandante de la totalidad o parte de los documentos, objetos, materiales, sustancias, ficheros electrónicos y cualesquiera otros soportes que contengan el secreto empresarial, y en su caso su destrucción total o parcial.

f) La atribución en propiedad de las mercancías infractoras al demandante, en cuyo caso el valor de las mercancías entregadas podrá imputarse al importe de la indemnización de daños y perjuicios debida, sin perjuicio de la subsistencia de la responsabilidad del infractor en lo que se refiere a la cuantía indemnizatoria que exceda del referido valor. Si el valor de las mercancías excede del importe de la indemnización, el demandante deberá compensarlo a la otra parte.

g) La indemnización de los daños y perjuicios, si ha intervenido dolo o culpa del infractor, que será adecuada respecto de la lesión realmente sufrida como consecuencia de la violación del secreto empresarial.

h) La publicación o difusión completa o parcial de la sentencia, que deberá preservar en todo caso la confidencialidad del secreto empresarial en los términos del artículo 15 de esta ley.

2. Las medidas adoptadas en virtud de las letras d), e) y h) del apartado anterior se ejecutarán a expensas del infractor, salvo que por excepción haya motivos para que deba ser de otro modo, y no restringen el derecho a la indemnización de daños y perjuicios que pueda ostentar el demandante.

3. Para determinar las medidas que se acuerden por virtud de las acciones del apartado 1, se tendrá en cuenta su proporcionalidad y las circunstancias del caso, y entre ellas el valor y otras características del secreto empresarial en cuestión, las medidas adoptadas para su protección, el comportamiento del infractor, las consecuencias de la violación del secreto empresarial, la probabilidad de que el infractor persista en la violación, los intereses legítimos de las partes, las consecuencias que podría tener para las partes que se estimen o no las acciones ejercitadas, los intereses legítimos de terceros, el interés público y la salvaguarda de los derechos fundamentales.

A los efectos de la publicación o difusión de la sentencia, los jueces y tribunales también tendrán en cuenta si la información relativa al infractor permitiría identificar a una persona física y, de ser así, si se justifica la publicación de dicha información, atendiendo, en particular, al posible perjuicio que esa medida pudiera ocasionar a la intimidad y reputación del infractor condenado.

4. Cuando la sentencia limite la duración de la cesación y prohibición que ordene, dicha duración deberá ser suficiente para eliminar cualquier ventaja competitiva o económica que el infractor hubiera podido extraer de la violación del secreto empresarial.

5. Las medidas de cesación y prohibición dejarán de tener efecto, a instancia de parte, cuando la información en cuestión deje de constituir un secreto empresarial por causas que no puedan atribuirse directa o indirectamente al infractor condenado.

6. En los supuestos de las letras a) a f) del apartado 1, la sentencia fijará, si así hubiera sido solicitado por el actor, la cuantía líquida de una indemnización coercitiva a favor del demandante, adecuada a las circunstancias, por día transcurrido hasta que se produzca el cumplimiento de la sentencia. Su importe se acumulará al que corresponda percibir al demandante con carácter general. Al solicitar la ejecución se podrá pedir que se entienda ampliada a los sucesivos incumplimientos, en los términos previstos en el artículo 578 de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.

7. A petición de la parte demandada, cuando sea un tercer adquirente de buena fe, las medidas objeto de las acciones del apartado 1 podrán sustituirse por el pago a favor de la parte demandante de una indemnización pecuniaria, siempre que ésta resulte razonablemente satisfactoria y la ejecución de aquellas medidas hubiera de causar a la parte

demandada un perjuicio desproporcionado. La indemnización pecuniaria que sustituya a la cesación o prohibición no excederá del importe que habría habido que pagar al titular del secreto empresarial por la concesión de una licencia que habría permitido utilizarlo durante el período en el que su utilización hubiera podido prohibirse.

Artículo 10. *Cálculo de los daños y perjuicios.*

1. Al fijarse la indemnización de daños y perjuicios se tendrán en cuenta todos los factores pertinentes, como son los perjuicios económicos, incluido el lucro cesante, que haya sufrido el titular del secreto empresarial, el enriquecimiento injusto obtenido por el infractor y, cuando proceda, otros elementos que no sean de orden económico, como el perjuicio moral causado al titular del secreto empresarial por su obtención, utilización o revelación ilícitas. También podrán incluirse, en su caso, los gastos de investigación en los que se haya incurrido para obtener pruebas razonables de la comisión de la infracción objeto del procedimiento judicial.

Con carácter alternativo, se podrá fijar, según los casos, una cantidad a tanto alzado en concepto de indemnización de daños y perjuicios, atendiendo, al menos y entre otros aspectos, al importe que la parte demandada habría tenido que pagar al titular del secreto empresarial por la concesión de una licencia que le hubiera permitido utilizarlo durante el período en el que su utilización podría haberse prohibido.

2. En relación con el cálculo y liquidación de los daños y perjuicios, será de aplicación lo dispuesto en el artículo 73 de la Ley de Patentes. Asimismo, las diligencias para este fin se llevarán a cabo a partir de las bases fijadas en la sentencia conforme al procedimiento previsto en el Capítulo IV del Título V del Libro III de la Ley de Enjuiciamiento Civil.

Artículo 11. *Prescripción.*

Las acciones de defensa de los secretos empresariales prescriben por el transcurso de tres años desde el momento en que el legitimado tuvo conocimiento de la persona que realizó la violación del secreto empresarial. Su prescripción se interrumpirá por las causas previstas con carácter general en el Código Civil.

CAPÍTULO V

Jurisdicción y normas procesales

Sección 1.ª Disposiciones generales

Artículo 12. *Jurisdicción y procedimiento.*

Los litigios civiles que puedan surgir al amparo de la presente ley se conocerán por los jueces y tribunales del orden jurisdiccional civil y se resolverán en el juicio que corresponda conforme a la Ley de Enjuiciamiento Civil.

Artículo 13. *Legitimación para el ejercicio de las acciones.*

1. Estarán legitimados para el ejercicio de las acciones de defensa previstas en esta ley el titular del secreto empresarial y quienes acrediten haber obtenido una licencia exclusiva o no exclusiva para su explotación que les autorice expresamente dicho ejercicio.

2. El titular de una licencia exclusiva o no exclusiva para la explotación de un secreto empresarial que no esté legitimado para el ejercicio de las acciones de defensa según lo dispuesto en el apartado anterior, podrá requerir fehacientemente al titular del mismo para que entable la acción judicial correspondiente. Si el titular se negara o no ejercitara la oportuna acción dentro de un plazo de tres meses, podrá el licenciatario entablarla en su propio nombre, acompañando el requerimiento efectuado. Con anterioridad al transcurso del plazo mencionado, el licenciatario podrá pedir al juez la adopción de medidas cautelares urgentes cuando justifique la necesidad de las mismas para evitar un daño importante, con presentación del referido requerimiento.

3. El licenciatario que ejercite una acción en virtud de lo dispuesto en alguno de los apartados anteriores deberá notificárselo fehacientemente al titular del secreto empresarial,

el cual podrá personarse e intervenir en el procedimiento, ya sea como parte en el mismo o como coadyuvante.

Artículo 14. *Competencia.*

Será territorialmente competente para conocer de las acciones previstas en esta ley el Juzgado de lo Mercantil correspondiente al domicilio del demandado o, a elección del demandante, el Juzgado de lo Mercantil de la provincia donde se hubiera realizado la infracción o se hubieran producido sus efectos.

Artículo 15. *Tratamiento de la información que pueda constituir secreto empresarial.*

1. Las partes, sus abogados o procuradores, el personal de la Administración de Justicia, los testigos, los peritos y cualesquiera otras personas que intervengan en un procedimiento relativo a la violación de un secreto empresarial, o que tengan acceso a documentos obrantes en dicho procedimiento por razón de su cargo o de la función que desempeñan, no podrán utilizar ni revelar aquella información que pueda constituir secreto empresarial y que los jueces o tribunales, de oficio o a petición debidamente motivada de cualquiera de las partes, hayan declarado confidencial y del que hayan tenido conocimiento a raíz de dicha intervención o de dicho acceso.

Esta prohibición estará en vigor incluso tras la conclusión del procedimiento, salvo que por sentencia firme se concluya que la información en cuestión no constituye secreto empresarial o, con el tiempo, pase a ser de conocimiento general o fácilmente accesible en los círculos en que normalmente se utilice.

2. Los jueces y tribunales podrán asimismo, de oficio o previa solicitud motivada de una de las partes, adoptar las medidas concretas necesarias para preservar la confidencialidad de la información que pueda constituir secreto empresarial y haya sido aportada a un procedimiento relativo a la violación de secretos empresariales o a un procedimiento de otra clase en el que sea necesaria su consideración para resolver sobre el fondo.

Las medidas a las que se refiere el párrafo anterior podrán incluir, entre otras que sean adecuadas y proporcionadas, las siguientes:

a) Restringir a un número limitado de personas el acceso a cualquier documento, objeto, material, sustancia, fichero electrónico u otro soporte que contenga información que pueda constituir en todo o en parte secreto empresarial;

b) Restringir a un número limitado de personas el acceso a las vistas, cuando en ellas pueda revelarse información que pueda constituir en todo o en parte secreto empresarial, así como el acceso a las grabaciones o transcripciones de estas vistas;

c) Poner a disposición de toda persona que no esté incluida entre el limitado número de personas al que se hace referencia en las letras a) y b) una versión no confidencial de la resolución judicial que se dicte, de la que se hayan eliminado o en la que se hayan ocultado los pasajes que contengan información que pueda constituir secreto empresarial.

La determinación del número de personas al que se hace referencia en las letras a) y b) de este apartado habrá de respetar el derecho de las partes a la tutela judicial efectiva y a un juez imparcial, e incluirá, al menos, una persona física de cada una de las partes y sus respectivos abogados y procuradores.

En todo caso, la adopción, contenido y circunstancias de las medidas para preservar la confidencialidad de la información previstas en este apartado tendrá en cuenta los intereses legítimos de las partes y de los terceros así como el perjuicio que pudiera ocasionárseles, y habrá de respetar el derecho de las partes a la tutela judicial efectiva y a un juez imparcial.

3. Todo tratamiento de datos de carácter personal que deba efectuarse en virtud de los apartados precedentes se llevará a cabo de conformidad con la normativa de la Unión Europea y española en materia de protección de datos de carácter personal.

Artículo 16. *Incumplimiento de la buena fe procesal.*

Los intervinientes en procesos de acciones por violación de secretos empresariales deberán ajustarse a las reglas de la buena fe procesal en los términos previstos en el artículo 247 de la Ley de Enjuiciamiento Civil. Como especialidad frente a lo estipulado en el

apartado 3 de dicho artículo, la multa que podrá imponerse a la parte demandante que haya ejercido la acción de forma abusiva o de mala fe, podrá alcanzar, sin otro límite, la tercera parte de la cuantía del litigio, tomándose en consideración a los efectos de su fijación, entre otros criterios, la gravedad del perjuicio ocasionado, la naturaleza e importancia de la conducta abusiva o de mala fe, la intencionalidad y el número de afectados. Además, los jueces y tribunales podrán ordenar la difusión de la resolución en que se constate ese carácter abusivo y manifiestamente infundado de la demanda interpuesta.

Sección 2.ª Diligencias para la preparación del ejercicio de acciones de defensa de los secretos empresariales

Artículo 17. *Diligencias de comprobación de hechos.*

Quien vaya a ejercitar una acción civil de defensa de secretos empresariales podrá solicitar del Juzgado de lo Mercantil que haya de entender de ella la práctica de diligencias de comprobación de aquellos hechos cuyo conocimiento resulte indispensable para preparar la correspondiente demanda. Estas diligencias de comprobación se regirán por lo previsto en el Capítulo II del Título XII de la Ley de Patentes.

Artículo 18. *Acceso a fuentes de prueba.*

Quien ejercite o vaya a ejercitar una acción civil de defensa de secretos empresariales podrá solicitar del Juzgado de lo Mercantil que haya de entender de ella la adopción de medidas de acceso a fuentes de prueba por los cauces previstos en los artículos 283 bis a) a 283 bis h) y 283 bis k), de la Ley de Enjuiciamiento Civil.

Artículo 19. *Medidas de aseguramiento de la prueba.*

Quien ejercite o vaya a ejercitar una acción civil de defensa de secretos empresariales podrá solicitar del Juzgado de lo Mercantil que haya de entender de ella, de conformidad con el artículo 297 de la Ley de Enjuiciamiento Civil, la adopción de las medidas de aseguramiento de la prueba que se consideren oportunas, en particular las mencionadas en el párrafo segundo del apartado 2 del citado artículo.

Sección 3.ª Medidas cautelares

Artículo 20. *Petición y régimen de las medidas cautelares.*

Quien ejercite o vaya a ejercitar una acción civil de defensa de secretos empresariales podrá solicitar del órgano judicial que haya de entender de ella la adopción de medidas cautelares tendentes a asegurar la eficacia de dicha acción, que se regirán por lo previsto en esta ley y, en lo demás, por lo dispuesto en el Capítulo III del Título XII de la Ley de Patentes y en el Título VI del Libro III de la Ley de Enjuiciamiento Civil.

Artículo 21. *Posibles medidas cautelares.*

Podrán adoptarse como medidas cautelares contra el presunto infractor las que aseguren debidamente la completa efectividad del eventual fallo que en su día recaiga y, en especial, las siguientes:

a) El cese o, en su caso, prohibición de utilizar o revelar el secreto empresarial;
b) El cese o, en su caso, prohibición de producir, ofrecer, comercializar o utilizar mercancías infractoras o de importar, exportar o almacenar mercancías infractoras con tales fines;
c) La retención y depósito de mercancías infractoras;
d) El embargo preventivo de bienes, para el aseguramiento de la eventual indemnización de daños y perjuicios.

Artículo 22. *Presupuestos.*

Al verificar la concurrencia de los presupuestos generales de las medidas cautelares, el tribunal habrá de examinar especialmente las circunstancias específicas del caso y su

proporcionalidad teniendo en cuenta el valor y otras características del secreto empresarial, las medidas adoptadas para protegerlo, el comportamiento de la parte contraria en su obtención, utilización o revelación, las consecuencias de su utilización o revelación ilícitas, los intereses legítimos de las partes y las consecuencias para estas de la adopción o de la falta de adopción de las medidas, los intereses legítimos de terceros, el interés público y la necesidad de salvaguardar los derechos fundamentales.

Artículo 23. *Solicitud de caución sustitutoria por el demandado.*

El demandado podrá solicitar la sustitución de la efectividad de las medidas cautelares acordadas por la prestación por su parte de una caución suficiente, de conformidad con lo dispuesto en el artículo 129 de la Ley de Patentes y en los artículos 746 y 747 de la Ley de Enjuiciamiento Civil.

Como excepción, en ningún caso se admitirá que el demandado sustituya por caución las medidas cautelares dirigidas a evitar la revelación de secretos empresariales.

Artículo 24. *Alzamiento de las medidas cautelares en caso de desaparición sobrevenida del secreto empresarial.*

A instancia de la parte demandada se alzarán las medidas cautelares previstas en las letras a), b) y c) del artículo 21 si la información en relación con la cual se interpuso la demanda ha dejado de reunir los requisitos para ser considerada secreto empresarial, por motivos que no puedan imputarse a aquella.

Artículo 25. *Caución exigible al demandante.*

1. El solicitante de la medida cautelar deberá prestar caución suficiente para responder, de manera rápida y efectiva, de los daños y perjuicios que la adopción de la medida cautelar pudiera causar al patrimonio del demandado, de conformidad con lo dispuesto en el artículo 728.3 de la Ley de Enjuiciamiento Civil.

2. A los efectos de determinar la caución, el tribunal habrá de valorar los potenciales perjuicios que las medidas cautelares puedan ocasionar a los terceros que resulten afectados desfavorablemente por aquellas. A los efectos de lo dispuesto en el apartado siguiente, no podrá cancelarse la caución en tanto no haya transcurrido un año desde el alzamiento de las medidas cautelares.

3. Los terceros que hayan resultado afectados desfavorablemente por las medidas cautelares adoptadas en virtud de lo dispuesto en esta sección y que hayan sido alzadas debido a un acto u omisión del demandante, o por haberse constatado posteriormente que la obtención, utilización o revelación del secreto empresarial no fueron ilícitas o no existía riesgo de tal ilicitud, podrán reclamar la indemnización de los daños y perjuicios conforme a lo establecido en el Capítulo IV del Título V del Libro III de la Ley de Enjuiciamiento Civil, aun no habiendo sido parte en el proceso declarativo. En tal caso, podrán solicitar que la caución a que se refiere el apartado anterior se mantenga, total o parcialmente, en tanto no se dicte resolución, siempre que la solicitud de indemnización se interponga dentro del plazo establecido en el apartado anterior.

Disposición transitoria única. *Régimen transitorio.*

1. La presente ley será de aplicación para la protección de cualesquiera secretos empresariales, con independencia de la fecha en que se hubiere adquirido legítimamente la titularidad sobre ellos.

2. Las acciones de defensa de los secretos empresariales que se hubieran iniciado antes de la entrada en vigor de esta ley se seguirán por el mismo procedimiento con arreglo al cual se hubieran incoado.

Disposición final primera. *Modificación de la Ley 17/1985, de 1 de julio, sobre objetos fabricados con materiales preciosos.*

El artículo trece de la Ley 17/1985, de 1 de julio, sobre objetos fabricados con metales preciosos, queda redactado como sigue:

«Artículo trece.

1. Para la comercialización en el territorio español de objetos fabricados con metales preciosos importados procedentes de Estados que no sean Miembro de la Unión Europea, se exigen los siguientes requisitos:

a) Que cumplan los requisitos que para la comercialización en el mercado interior se establecen en el Capítulo II de esta Ley.

b) Que con independencia de los contrastes con que estos objetos hayan sido marcados en el Estado de origen, y aunque incorporen contrastes de garantía aplicados por entidades de un Estado Miembro de la Unión Europea con legislación equivalente, deben ser marcados en destino con el punzón de contraste de garantía, efectuado por un laboratorio de contraste reconocido en España.

En ningún caso se reconocen los contrastes efectuados por laboratorios *off-shore* incluso aunque estos laboratorios hayan sido habilitados por Estados Miembro de la Unión Europea con legislación equivalente a la española.

2. Los objetos fabricados con metales preciosos procedentes de otro Estado Miembro de la Unión Europea, con legislación equivalente a la española, podrán ser comercializados en el territorio español sin necesidad de cumplir los requisitos previstos en el apartado 1 del presente artículo, siempre que posean el contraste de identificación de origen y el contraste de garantía del Estado Miembro de procedencia, y que estos contrastes cumplan los siguientes requisitos:

a) El contraste de identificación de origen deberá haber sido registrado por el órgano correspondiente del Estado Miembro de procedencia.

b) El contraste de garantía que ofrecerá una información equivalente a la exigida por la presente Ley a tales contrastes.

Asimismo, deberá haber sido realizado por un organismo independiente o, en su caso, por un laboratorio sometido al control de la Administración pública o de un organismo independiente de un Estado Miembro.

3. En el caso de que los objetos fabricados con metales preciosos sean procedentes de otro Estado Miembro de la Unión Europea, con legislación no equivalente a la española, les serán de aplicación lo previsto en el apartado 1 del presente artículo, salvo que concurriera la circunstancia prevista en el apartado 4.

En el caso en el que el Estado Miembro tuviera un sistema de contraste voluntario a priori, y si el objeto ha pasado el control del laboratorio u organismo independiente habilitado en el citado Estado a tal efecto y dispone de contraste de garantía, no tiene que ser contrastado de nuevo por un laboratorio español oficial o autorizado.

En ningún caso se reconocen los contrastes de objetos fabricados con metales preciosos efectuados por los laboratorios habilitados en un Estado Miembro con legislación no equivalente por otros Estados Miembro de la Unión Europea con legislación equivalente a la española (laboratorios *off-shore).*

4. No serán de aplicación las previsiones de los apartados 1, 2 y 3 del presente artículo si existiesen acuerdos con otro u otros Estados sobre condiciones de reconocimiento mutuo de contrastes de objetos fabricados con metales preciosos.»

Disposición final segunda. *Modificación de la Ley 3/1991, de 10 de enero, de Competencia Desleal.*

El artículo 13 de la Ley 3/1991, de 10 de enero, de Competencia Desleal queda redactado como sigue:

«Artículo 13. *Violación de secretos.*

Se considera desleal la violación de secretos empresariales, que se regirá por lo dispuesto en la legislación de secretos empresariales.»

Disposición final tercera. *Habilitación para aprobar un texto refundido de la Ley 22/2003, de 9 de julio, Concursal.*

Al objeto de consolidar en un texto único las modificaciones incorporadas desde su entrada en vigor a la Ley 22/2003, de 9 de julio, Concursal, se autoriza al Gobierno para elaborar y aprobar, a propuesta de los Ministros de Justicia y de Economía y Empresa, en un plazo de ocho meses a contar desde la entrada en vigor de la presente ley, un texto refundido de la citada norma. Esta autorización incluye la facultad de regularizar, aclarar y armonizar los textos legales que deban ser refundidos.

Disposición final cuarta. *Título competencial.*

Esta ley se dicta al amparo de la competencia estatal prevista por el artículo 149.1.9.ª de la Constitución en materia de legislación sobre propiedad industrial, salvo los artículos 1.3 y 2.3.c), que se dictan al amparo del artículo 149.1.7.ª de la Constitución, que reconoce la competencia estatal sobre la legislación laboral, y el Capítulo V que se ampara en el artículo 149.1.6.ª de la Constitución que atribuye al Estado la competencia sobre legislación procesal.

Disposición final quinta. *Incorporación de Derecho de la Unión Europea.*

Mediante esta ley se incorpora al Derecho español la Directiva (UE) 2016/943 del Parlamento Europeo y del Consejo, de 8 de junio de 2016, relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas.

Disposición final sexta. *Entrada en vigor.*

La presente ley entrará en vigor a los veinte días de su publicación en el «Boletín Oficial del Estado».

§ 19

Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional

Ministerio de la Presidencia, Relaciones con las Cortes e Igualdad
«BOE» núm. 103, de 30 de abril de 2019
Última modificación: sin modificaciones
Referencia: BOE-A-2019-6347

El Consejo de Seguridad Nacional, en su reunión del día 12 de abril de 2019, ha aprobado la Estrategia Nacional de Ciberseguridad 2019.

Para general conocimiento se dispone su publicación en el «Boletín Oficial del Estado» como anexo a la presente Orden.

ANEXO

Estrategia Nacional de Ciberseguridad 2019

Sumario

Presidencia del Gobierno.
Consejo de Seguridad Nacional.
Sumario.
Resumen ejecutivo.
Introducción.
Capítulo 1: El ciberespacio como espacio común global.
El ciberespacio: oportunidades y desafíos.
Infraestructura digital.
Plano internacional: seguridad en el ciberespacio.
Una nueva concepción del ciberespacio.
Capítulo 2: Las amenazas y desafíos en el ciberespacio.
Ciberamenazas.
Acciones que usan el ciberespacio para fines maliciosos.
Capítulo 3: Propósito, principios y objetivos para la ciberseguridad.
Propósito.
Principios Rectores.
Objetivo general.
Objetivo I.
Objetivo II.
Objetivo III.
Objetivo IV.

Objetivo V.
Capítulo 4: Líneas de acción y medidas.
Línea de acción 1.
Línea de acción 2.
Línea de acción 3.
Línea de acción 4.
Línea de acción 5.
Línea de acción 6.
Línea de acción 7.
Capítulo 5: La ciberseguridad en el Sistema de Seguridad Nacional.
El Consejo de Seguridad Nacional.
El Comité de Situación.
El Consejo Nacional de Ciberseguridad.
La Comisión Permanente de Ciberseguridad.
Foro Nacional de Ciberseguridad.
Autoridades públicas competentes y los CSIRT de referencia nacionales.
Consideraciones finales y evaluación.

Resumen ejecutivo

La Estrategia Nacional de Ciberseguridad desarrolla las previsiones de la Estrategia de Seguridad Nacional de 2017 en el ámbito de la ciberseguridad, considerando los objetivos generales, el objetivo del ámbito y las líneas de acción establecidas para conseguirlo.

El documento se estructura en cinco capítulos. El primero, titulado «El ciberespacio, más allá de un espacio común global», proporciona una visión de conjunto del ámbito de la ciberseguridad, los avances realizados en materia la materia desde la aprobación de la Estrategia de 2013, las razones que afianzan la elaboración de la Estrategia Nacional de Ciberseguridad 2019, así como las principales características que impulsan su desarrollo.

Las actividades que se desarrollan en el ciberespacio son fundamentales para la sociedad actual. La tecnología e infraestructuras que forman parte del ciberespacio son elementos estratégicos, transversales a todos los ámbitos de actividad, siendo la vulnerabilidad del ciberespacio una de los principales riesgos para nuestro desarrollo como nación.

Por ello, la seguridad en el ciberespacio es un objetivo prioritario en las agendas de los gobiernos con el fin de garantizar su Seguridad Nacional y una competencia del Estado para crear una sociedad digital en la que la confianza es un elemento fundamental.

Contribuir a la promoción de un ciberespacio seguro y fiable, desde un enfoque multidisciplinar abarcando aspectos más allá de los puramente técnicos, es una tarea que debe partir del conocimiento y comprensión de las amenazas a las que nos podemos enfrentar, incluyendo nuevas y emergentes.

El segundo capítulo, titulado «Las amenazas y desafíos en el ciberespacio» determina las principales amenazas del ciberespacio que derivan de su condición de espacio global común, de la elevada tecnificación y de la gran conectividad que posibilita la amplificación del impacto ante cualquier ataque. Clasifica estas amenazas y desafíos en dos categorías: por un lado, las que amenazan a activos que forman parte del ciberespacio; y por otro, aquellos que usan el ciberespacio como medio para realizar actividades maliciosas e ilícitas de todo tipo.

El tercer capítulo, titulado «Propósito, principios y objetivos para la ciberseguridad» aplica los principios rectores de la Estrategia de Seguridad Nacional 2017 (Unidad de acción, Anticipación, Eficiencia y Resiliencia) a cinco objetivos específicos. Su desarrollo, se plasma en el cuarto capítulo titulado «Líneas de acción y medidas», donde se establecen siete líneas de acción y se identifican las medidas para el desarrollo de cada una de ellas.

Dichas líneas de acción se dirigen a: reforzar las capacidades ante las amenazas provenientes del ciberespacio; garantizar la seguridad y resiliencia de los activos estratégicos para España; impulsar la ciberseguridad de ciudadanos y empresas; reforzar las capacidades de investigación y persecución de la cibercriminalidad, para garantizar la seguridad ciudadana y la protección de los derechos y libertades en el ciberespacio;

impulsar la ciberseguridad de ciudadanos y empresas; potenciar la industria española de ciberseguridad, y la generación y retención de talento, para el fortalecimiento de la autonomía digital; contribuir a la seguridad del ciberespacio en el ámbito internacional, promoviendo un ciberespacio abierto, plural, seguro y confiable en apoyo de los intereses nacionales y desarrollar una cultura de ciberseguridad de manera que se contribuya al Plan Integral de Cultura de Seguridad Nacional.

El quinto capítulo, titulado «La ciberseguridad en el Sistema de Seguridad Nacional» define la arquitectura orgánica de la ciberseguridad. Bajo la dirección del Presidente del Gobierno, la estructura se compone de tres órganos: el Consejo de Seguridad Nacional, como Comisión Delegada del Gobierno para la Seguridad Nacional; el Consejo Nacional de Ciberseguridad, que apoya al Consejo de Seguridad Nacional y asiste al Presidente del Gobierno en la dirección y coordinación de la política de Seguridad Nacional en el ámbito de la ciberseguridad, y fomenta las relaciones de coordinación, colaboración y cooperación entre Administraciones Públicas y entre estas y el sector privado, y el Comité de Situación que, con el apoyo del Departamento de Seguridad Nacional, apoyará a la gestión de las situaciones de crisis en cualquier ámbito, que por su transversalidad o dimensión, desborden las capacidades de respuesta de los mecanismos habituales.

Se complementa este sistema con la Comisión Permanente de Ciberseguridad, que facilita la coordinación interministerial a nivel operacional en el ámbito de la ciberseguridad, siendo el órgano que asistirá al Consejo Nacional de Ciberseguridad sobre aspectos relativos a la valoración técnica y operativa de los riesgos y amenazas a la ciberseguridad; las autoridades públicas competentes y CSIRT (Computer Security Incident Response Team) de referencia nacional, y se incorpora la creación de un elemento novedoso de colaboración público privada, el foro Nacional de Ciberseguridad.

Asimismo, en este último capítulo, se exponen a modo de conclusión, unas consideraciones finales y se concretan los mecanismos para la actualización y evaluación de la Estrategia.

Introducción

La Estrategia Nacional de Ciberseguridad 2019 establece la posición de España ante una nueva concepción de la ciberseguridad en el marco de la Política de Seguridad Nacional.

En 2013 se aprobó la primera Estrategia Nacional de Ciberseguridad en España. El documento fijaba las directrices y líneas generales de actuación para hacer frente al desafío que supone, para el país, la vulnerabilidad del ciberespacio. Además, la estrategia diseñaba el modelo de gobernanza para la ciberseguridad nacional. Igualmente, en estos años, España ha seguido avanzando en sus esfuerzos por contribuir a la promoción de un ciberespacio seguro y fiable.

Uno de sus pilares, creado en el año 2014, es el Consejo Nacional de Ciberseguridad, órgano de apoyo del Consejo de Seguridad Nacional. Desde su primera reunión, el Consejo Nacional de Ciberseguridad ha asumido la tarea de coordinar los organismos con competencia en la materia a nivel nacional y el desarrollo del Plan Nacional de Ciberseguridad y sus planes derivados. Así, hoy España cuenta con organismos especializados en ciberseguridad y una posición destacada a nivel europeo e internacional.

El marco jurídico también ha experimentado una notable adaptación. En respuesta a su evolución y a la experiencia acumulada en estos años, en 2015 se publicó la modificación del Esquema Nacional de Seguridad para garantizar la seguridad de los sistemas del Sector Público. Por otro lado, la entrada en vigor del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, que transpone al ordenamiento jurídico español la Directiva (UE) 2016/1148 (conocida como Directiva NIS), ha supuesto un importante hito en la mejora de la ciberseguridad en nuestro país, extendiendo el alcance de esta Directiva con el objetivo de mejorar la ciberseguridad de todos los sectores estratégicos.

La Ley 36/2015, de 28 de septiembre, de Seguridad Nacional se promulgó con vocación de dar impulso a uno de los proyectos de mayor responsabilidad para un gobierno, la Seguridad Nacional. La Ley de Seguridad Nacional contempla la ciberseguridad como ámbito de especial interés.

Se puede afirmar, sin lugar a dudas, que la ciberseguridad ha modernizado la Seguridad Nacional, tratándose de uno de los ámbitos de mayor avance hasta la fecha. Esta dinámica debe seguir su camino adelante.

La Estrategia de Seguridad Nacional 2017 marca un punto de inflexión en el pensamiento estratégico nacional, donde la ciberseguridad debe ocupar un espacio propio y diferencial.

Una de las tendencias globales identificadas en la Estrategia, la digitalización, se muestra como motor del cambio con implicaciones para la seguridad. La Estrategia establece un esquema novedoso, con cinco objetivos generales que resultan transversales a todos los ámbitos. La gestión de crisis, la cultura de Seguridad Nacional, los espacios comunes globales, el desarrollo tecnológico y la proyección internacional de España conforman una matriz estratégica donde la ciberseguridad está llamada a abrir nuevas vías hacia el modelo de presente y futuro de la seguridad en España.

La nueva ciberseguridad se extiende más allá del campo meramente de la protección del patrimonio tecnológico para adentrarse en las esferas política, económica y social.

Además de las acciones para causar efectos en los sistemas digitales, se debe tener en cuenta la concepción del ciberespacio como un vector de comunicación estratégica, que puede ser utilizado para influir en la opinión pública y en la forma de pensar de las personas a través de la manipulación de la información, las campañas de desinformación o las acciones de carácter híbrido. Su potencial aplicación en situaciones muy diversas, donde se incluyen los procesos electorales, genera un elevado grado de complejidad.

Ante esta visión renovada de un ámbito que se entiende extendido funcionalmente, y para el que la colaboración público-privada es un elemento clave, resulta necesaria una nueva aproximación, una nueva estrategia nacional de ciberseguridad.

CAPÍTULO 1

El ciberespacio como espacio común global

Este capítulo presenta las oportunidades y desafíos del ciberespacio y la infraestructura digital, expone el carácter inherentemente internacional de la aproximación a su seguridad y describe los principales rasgos de la nueva concepción de la ciberseguridad en España.

El ciberespacio: oportunidades y desafíos:

El ciberespacio es un espacio común global caracterizado por su apertura funcional y su dinamismo. La ausencia de soberanía, su débil jurisdicción, la facilidad de acceso y la dificultad de atribución de las acciones que en él se desarrollan definen un escenario que ofrece innumerables oportunidades de futuro, aunque también presenta serios desafíos a la seguridad.

Por una parte, el ciberespacio posibilita la conectividad universal y facilita el libre flujo de información, servicios e ideas. Se constituye así en un ámbito que estimula el emprendimiento, potencia el progreso socioeconómico y ofrece cada día nuevas posibilidades en todos los sectores de actividad. El cambio que la transformación digital provoca en los procesos productivos se manifiesta a escala global y a un ritmo sin precedentes. La inteligencia artificial, la robótica, el big data, el blockchain y el internet de las cosas son ya una realidad, si bien el verdadero potencial transformador está todavía por descubrir. Sus implicaciones van más allá de la dimensión tecnológica, se extienden hacia nuevos modelos sociales y se adentran en el campo de las relaciones personales y la ética.

Por otra parte, la digitalización transforma la seguridad y presenta serios desafíos. El ciberespacio se configura como campo de batalla donde la información y la privacidad de los datos son activos de alto valor en un entorno de mayor competición geopolítica, reordenación del poder y empoderamiento del individuo. Así, la creciente conectividad y la mayor dependencia de las redes y sistemas, así como de componentes, objetos y dispositivos digitales, generan vulnerabilidades y dificultan la adecuada protección de la información.

Infraestructura digital:

Además de su naturaleza virtual, el ciberespacio se sustenta en elementos físicos y lógicos. Los dispositivos, componentes y sistemas que constituyen las redes y sistemas de información y comunicaciones están expuestos a disfunciones que alteran su correcto funcionamiento y a acciones deliberadas con fines malintencionados, que ponen en riesgo el funcionamiento de las infraestructuras críticas y de los servicios esenciales que dependen de los sistemas y redes digitales asociadas.

Este riesgo se ve amplificado por la prevalencia de criterios comerciales frente a los de seguridad en el diseño de los productos hardware y software, así como de los sistemas y de los servicios, algo que dificulta los procesos de certificación y puede comprometer la cadena de suministro.

Todos estos elementos, unidos a la creciente interconectividad entre sistemas pueden originar efectos en cascada con resultados impredecibles.

Plano internacional: seguridad en el ciberespacio:

La seguridad en el ciberespacio se ha convertido en un objetivo prioritario en las agendas de los gobiernos con el fin de garantizar su seguridad nacional y de crear una sociedad digital basada en la confianza. En este contexto, España defiende su visión e intereses como nación y contribuye al esfuerzo conjunto de la comunidad internacional en su apuesta por un ciberespacio abierto, plural y seguro.

España continúa participando activamente en todas las instituciones en las que la ciberseguridad ocupa un lugar destacado, en especial en el marco de la Unión Europea, la Alianza Atlántica y de Naciones Unidas, demostrando así el compromiso con sus socios y aliados. Asimismo, se mantienen vínculos con terceros Estados mediante mecanismos de cooperación bilateral que facilitan elementos de entendimiento y confianza mutua basados en las relaciones fluidas en el ámbito de la ciberseguridad y orientados hacia la construcción de capacidades.

Consciente de la importancia del multilateralismo, además del Derecho Internacional y las normas no vinculantes de comportamiento responsable de los Estados, se destaca el papel de La Carta de Naciones Unidas como principio de referencia para la prevención de conflictos, la cooperación y la estabilidad en el ciberespacio. La construcción de consensos y las medidas de fomento de confianza constituyen la base para su aplicación y puesta en práctica, así como los Tratados y Convenios Internacionales en los que España es parte.

Una nueva concepción del ciberespacio:

Es una dimensión fundamental para la estabilidad el preservar la defensa de los valores y principios constitucionales y democráticos, así como los derechos fundamentales de los ciudadanos en el ciberespacio, especialmente en la protección de sus datos personales, su privacidad, su libertad de expresión y el acceso a una información veraz y de calidad.

El buen entendimiento de este planteamiento, exige trabajar con un enfoque multidisciplinar que abarque aspectos más allá de los puramente técnicos, bajo el principio de dirección centralizada y ejecución coordinada, con la afectación de la ciberseguridad a la Seguridad Nacional como competencia del Estado.

En primer lugar, el sector privado juega un papel relevante como uno de los gestores y propietarios de los activos digitales de España, por lo que las capacidades de ciberseguridad del país residen en gran medida en las de sus empresas. Es por tanto necesario el apoyo, la promoción y la inversión en ciberseguridad para impulsar la competitividad y el crecimiento económico, a la vez que proporcionar un entorno digital seguro y fiable.

Por otra parte, se debe aspirar a incrementar la autonomía tecnológica mediante el fomento de una base industrial nacional de ciberseguridad, la I+D+i y la gestión del talento tecnológico. En efecto, el recurso humano continúa siendo un factor crítico. Existe una diferencia importante entre el número de puestos de trabajo para los que es necesaria una alta especialización en las tecnologías de la información, en concreto en ciberseguridad, y las personas disponibles con el nivel de conocimiento o de formación requerida.

En segundo lugar, la transición de un modelo de ciberseguridad de carácter preventivo y defensivo hacia un esquema que incorpore elementos de mayor fuerza disuasoria obedece a un contexto global de mayor competencia geopolítica. El empleo del ciberespacio como dominio de confrontación, de forma independiente o como parte de una acción híbrida, es un

rasgo ampliamente reconocido. La disuasión en ciberseguridad requiere la obtención y potenciación de capacidades de ciberdefensa, como elemento fundamental de la acción del Estado.

En tercer lugar, la rápida evolución de las ciberamenazas aconseja una aproximación más proactiva de la ciberinteligencia. Su integración en el esquema conjunto de la ciberseguridad es un elemento clave para el conocimiento de la situación y la necesaria alerta temprana que permita anticiparse a las acciones de los potenciales adversarios a través del conocimiento de sus capacidades, técnicas, tácticas e intenciones. Así mismo, es necesario fomentar el empleo de mecanismos y medios que permitan una oportuna investigación y persecución de los autores para incrementar las posibilidades de atribución.

A todo lo anterior se une la necesidad de una mayor implicación de toda la sociedad mediante el fomento de una cultura de ciberseguridad, para evolucionar desde la concienciación al compromiso, en el entendimiento de que el ciudadano es corresponsable de la ciberseguridad nacional.

CAPÍTULO 2

Las amenazas y desafíos en el ciberespacio

En este capítulo se examinan las principales amenazas y desafíos del ciberespacio a los que se enfrenta España.

La promoción de un entorno seguro y fiable es una tarea que debe partir del conocimiento y la comprensión de los desafíos y las amenazas, incluyendo las nuevas y emergentes que afectan al ciberespacio. La Estrategia de Seguridad Nacional de 2017 diferencia entre las ciberamenazas y las acciones que usan el ciberespacio como medio para realizar actividades maliciosas o ilícitas.

Ciberamenazas:

Las ciberamenazas son todas aquellas disrupciones o manipulaciones maliciosas que afectan a elementos tecnológicos. Abarcan un amplio abanico de acciones. Las ciberamenazas se caracterizan por su diversidad tanto en lo que concierne a capacidades como a motivaciones. Afectan a la práctica totalidad de los ámbitos de la Seguridad Nacional, como la Defensa Nacional, la seguridad económica o la protección de las infraestructuras críticas, entre otros, y no distinguen fronteras.

Su carácter transversal, exige que la ciberseguridad sea afrontada con una perspectiva integral que comprenda a las Administraciones Públicas, al sector público y privado y a la sociedad en su conjunto, en tanto puede tener implicaciones simultáneas en aspectos tan diversos como la soberanía, los derechos fundamentales, la defensa, la economía y el desarrollo tecnológico.

En este escenario, las defensas deben evolucionar continuamente para ir adaptándose a una amenaza que lleva la iniciativa y que se multiplica por el efecto llamada que genera su alto grado de impunidad. Todo ello, mientras la superficie a defender se incrementa y complica cada día.

En este sentido, la seguridad de las redes y sistemas de información requiere potenciar las medidas de prevención, detección y respuesta, fomentando la seguridad por diseño y por defecto, que debe estar incorporada tanto en el desarrollo de productos y servicios tecnológicos, como en su actualización o manera de utilización.

Acciones que usan el ciberespacio para fines maliciosos:

Las tecnologías digitales dan entrada a nuevas actividades y formas de negocio que requieren ser debidamente reguladas, pues pueden afectar a la estabilidad y al ejercicio de derechos y libertades, presentando sustanciales amenazas y desafíos para la Seguridad Nacional. Igualmente, las mismas cualidades que hacen del ciberespacio un motor del progreso, pueden ser explotadas con fines perniciosos al sumarse a las excepcionales facilidades que concede para el anonimato, la suplantación y la amplificación.

Debido a la revolución de Internet, Estados, grupos organizados, colectivos y hasta individuos aislados pueden alcanzar un nivel de poder y una capacidad de influir impensable

en otros tiempos. La conectividad digital lleva a que los movimientos sociales globales tengan una importancia estratégica hasta hace poco subestimada.

Las acciones que usan el ciberespacio como medio para realizar actividades maliciosas o ilícitas incluyen las relacionadas con el ciberespionaje y la cibercriminalidad.

El ciberespionaje es un método relativamente económico, rápido y con menos riesgos que el espionaje tradicional, dada la dificultad de atribución de la autoría. Las mayores capacidades corresponden principalmente a actores estatales (organismos de inteligencia o militares), que fundamentalmente operan a través de las denominadas Amenazas Persistentes Avanzadas (APT). Un tipo de amenaza en la que el adversario posee sofisticados niveles de conocimiento y de recursos e infraestructuras para, mediante múltiples tipos de ataques, interactuar sobre sus objetivos por un extenso periodo de tiempo, adaptarse a los esfuerzos del defensor para resistir, así como mantener el nivel de interacción para ejecutar sus objetivos.

Asimismo, se constata una tendencia creciente de las denominadas amenazas híbridas, acciones coordinadas y sincronizadas dirigidas a atacar de manera deliberada las vulnerabilidades sistémicas de los estados democráticos y las instituciones, a través de una amplia gama de medios, tales como acciones militares tradicionales, ciberataques, operaciones de manipulación de la información, o elementos de presión económica. Actores estatales y no estatales, bien de forma directa o a través de intermediarios, explotan las facilidades que ofrece Internet para la desinformación y propaganda y un interés generalizado en la obtención y desarrollo de capacidades militares para operar en el ciberespacio, incluyendo en muchos casos capacidades ofensivas.

La cibercriminalidad, por su parte, es un problema de seguridad ciudadana de primer orden, representando una de las amenazas más extendidas y generalizadas, que se materializa de forma continua y que victimiza cada vez de manera más importante a miles de instituciones, empresas y ciudadanos. El término Cibercriminalidad, hace referencia al conjunto de actividades ilícitas cometidas en el ciberespacio que tienen por objeto los elementos, sistemas informáticos o cualesquiera otros bienes jurídicos, siempre que en su planificación, desarrollo y ejecución resulte determinante la utilización de herramientas tecnológicas; en función de la naturaleza del hecho punible en sí, de la autoría, de su motivación, o de los daños infligidos, se podrá hablar así de ciberterrorismo, de ciberdelito, o en su caso, de hacktivismo.

El empleo de nuevas modalidades de transacción financiera y económica, como las criptomonedas, para el tráfico y el comercio de bienes y prestación de servicios ilícitos o la extorsión, el fraude y la falsificación de medios de pago no monetarios, constituyen un serio desafío a la seguridad por su sofisticación y complejidad. Estos pueden ser utilizados en el blanqueo de capitales y la evasión de impuestos y representan una fuente de ingresos para el crimen organizado y por lo tanto son facilitadores de otras actividades como la financiación del terrorismo, que toma provecho de la dificultad de seguimiento que estas nuevas técnicas ofrecen.

Los ciberdelincuentes operan bajo esquemas de crimen organizado y continúan explorando de manera incesante técnicas sobre las que construir modelos de negocio lucrativo y de bajo riesgo, amparados por la difícil trazabilidad de sus acciones.

Los grupos terroristas tratan de aprovechar las vulnerabilidades del ciberespacio para realizar ciberataques o para actividades de radicalización de individuos y colectivos, financiación, divulgación de técnicas y herramientas para la comisión de atentados, y de reclutamiento, adiestramiento o propaganda. Íntimamente relacionado con ello, se halla la amenaza contra las infraestructuras críticas, con la posibilidad cierta de causar un colapso a través de las redes mediante una caída en cadena de los servicios esenciales.

Los grupos hacktivistas realizan ciberataques por razones ideológicas y, aprovechándose en ocasiones de productos, servicios y herramientas disponibles en el ciberespacio, buscan desarrollar ataques con un gran impacto mediático o social.

Tampoco se puede menospreciar la amenaza que entraña el incremento continuado de la contratación de servicios de cibercriminales, las organizaciones que buscan causar daño a sus competidores y los recursos tecnológicos y humanos internos que puedan resultar dañinos para las organizaciones, sin olvidar todas aquellas amenazas emergentes y las acciones resultantes de la falta de cultura de ciberseguridad.

Por otra parte, la información digital se ha convertido en un activo de alto valor añadido. El análisis de los datos personales que circulan en la red se aprovecha para múltiples fines que abarca desde estudios sociológicos hasta campañas comerciales. El empleo malintencionado de datos personales y las campañas de desinformación tienen un alto potencial desestabilizador en la sociedad, y la explotación de brechas en los datos personales supone una violación a la seguridad de dichos datos, que afecta a la privacidad de las personas y a la integridad y confidencialidad de sus datos.

En cuanto a las campañas de desinformación, hacen uso de elementos como las noticias falsas para influir en la opinión pública. Internet y las redes sociales amplifican el efecto y alcance de la información transmitida, con potencial aplicación en contra de objetivos como por ejemplo organizaciones internacionales, Estados, iniciativas políticas o personajes públicos o incluso a procesos electorales democráticos.

CAPÍTULO 3

Propósito, principios y objetivos para la ciberseguridad

En este capítulo se establece el propósito y los principios por los que se rige la Estrategia, así como los objetivos: uno general y cinco específicos.

Propósito:

España precisa, tal y como establece la Estrategia de Seguridad Nacional de 2017, garantizar un uso seguro y responsable de las redes y los sistemas de información y comunicaciones a través del fortalecimiento de las capacidades de prevención, detección y respuesta a los ciberataques potenciando y adoptando medidas específicas para un contribuir a la promoción de un ciberespacio seguro y fiable.

Por tanto, el propósito de la Estrategia Nacional de Ciberseguridad 2019, es fijar las directrices generales del ámbito de la ciberseguridad de manera que se alcancen los objetivos previstos en la Estrategia de Seguridad Nacional de 2017.

Para ello, España ha de seguir avanzando en el refuerzo de capacidades para hacer frente a las ciberamenazas y el uso malicioso del ciberespacio. En consecuencia, se seguirán promoviendo medidas que ayuden a garantizar a nuestra nación su seguridad, con especial atención al sector público y los servicios esenciales, en un marco más coordinado y con estructuras de cooperación mejoradas.

Por otra parte, el fomento de la cultura de ciberseguridad ha de ser uno de los ejes centrales a desarrollar a fin de contar con una sociedad más conocedora de las amenazas y desafíos a las que se enfrenta. El derecho a hacer un uso seguro y fiable del ciberespacio y el contribuir a que así sea, es una responsabilidad compartida.

Asimismo, la ciberseguridad es progreso, por lo que el apoyo e impulso de la industria española de ciberseguridad, la promoción de un entorno que favorezca la investigación, el desarrollo y la innovación, y la participación del mundo académico tiene un carácter singular. Por otro lado, es un objetivo prioritario en nuestra sociedad alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas y profesionales, ya que solo mediante su promoción se podrá responder a los grandes retos de la ciberseguridad.

La transversalidad y globalidad del ciberespacio, requiere además de la cooperación y del cumplimiento del Derecho internacional, del máximo respeto a los principios recogidos en la Constitución y en la Carta de Naciones Unidas; en coherencia con la Estrategia de Seguridad Nacional y con las iniciativas desarrolladas en el marco europeo, regional e internacional, prevaleciendo en todo momento los intereses nacionales.

Principios rectores:

La Estrategia Nacional de Ciberseguridad, se sustenta y se inspira en los principios rectores de la Seguridad Nacional: unidad de acción, anticipación, eficiencia y resiliencia.

Unidad de Acción: Toda respuesta ante un incidente en el ámbito de la ciberseguridad que pueda implicar a distintos agentes del Estado se verá reforzada si es coherente, coordinada y se resuelve de manera rápida y eficaz, cualidades alcanzables a través de la adecuada preparación y articulación de la unidad de acción del Estado.

Una gestión centralizada de las crisis que afecten al ciberespacio, permite mantener una visión completa de la situación de la amenaza y posibilita el empleo de los recursos disponibles de forma más rápida, eficiente, coherente e integral.

Anticipación: La especificidad del ciberespacio y de los actores implicados demanda que existan mecanismos de anticipación en organismos especializados que orienten la Acción del Estado en situaciones de crisis, y en la que igualmente deber participar el sector privado.

La anticipación prima las actuaciones preventivas sobre las reactivas. Disponer de sistemas eficaces, con información compartida lo más próximo al tiempo real, permite alcanzar un adecuado conocimiento de la situación. Dicho factor resulta imprescindible para minimizar el tiempo de respuesta, lo que puede resultar crítico para reducir los efectos de las amenazas.

Eficiencia: La ciberseguridad precisa del empleo de sistemas multipropósito de gran valor y elevado nivel tecnológico, que llevan asociadas unas necesidades muy exigentes y un alto coste derivado de su desarrollo, adquisición y operación. A lo anterior se suma la necesidad de una planificación anticipada y una elevada complejidad en su sostenimiento.

Además, el escenario actual y futuro está marcado por la austeridad económica, que unida a la responsabilidad social de obtener el máximo rendimiento de los recursos disponibles, obliga a orientar la acción del Estado hacia la optimización y la eficiencia de los dedicados a la ciberseguridad, por lo que resultarán indispensables la unidad de acción, compartición de información e integración de estos recursos para alcanzar la eficiencia deseada.

Resiliencia: La resiliencia es una característica fundamental que deben poseer los sistemas e infraestructuras críticas. El Estado está obligado a asegurar la disponibilidad de los elementos que se consideren esenciales para la nación, mejorando su protección contra las ciberamenazas. Especial mención merece el refuerzo que requieren las redes de información y comunicaciones frente a actividades de las ciberamenazas o al uso ilícito del ciberespacio.

Objetivo general:

Los nuevos retos de la ciberseguridad han requerido la adaptación de su objetivo general de manera que se muestre más integrador, inclusivo y menos tecnificado.

En línea con la Estrategia de Seguridad Nacional de 2017 y ampliando el objetivo para la ciberseguridad previsto en la misma, España garantizará el uso seguro y fiable del ciberespacio, protegiendo los derechos y las libertades de los ciudadanos y promoviendo el progreso socio económico.

Basados en este objetivo general, a continuación, se fijan una serie de objetivos específicos que orientan la acción del Estado en este ámbito.

Objetivo I

Seguridad y resiliencia de las redes y los sistemas de información y comunicaciones del sector público y de los servicios esenciales

Es necesario consolidar un marco nacional coherente e integrado que ayude a garantizar la protección de la información manejada por el sector público y por los servicios esenciales, sus sistemas y servicios, así como de las redes que los soportan. Este marco permitirá desarrollar e implantar servicios cada vez más seguros y eficientes.

Para ello, es necesario implantar medidas de seguridad enfocadas a mejorar las capacidades de prevención, detección y respuesta ante incidentes, desarrollando nuevas soluciones, reforzando la coordinación y adaptando en consecuencia el ordenamiento jurídico.

En particular, las acciones contra el ciberespionaje merecen especial mención para asegurar la protección del Patrimonio Tecnológico de España, entendido como aquellos activos materiales o inmateriales que sustentan la propiedad intelectual e industrial del sector empresarial, que conforman nuestro presente y condicionan el desarrollo futuro.

El sector público y los operadores de servicios esenciales se deben involucrar activamente en un proceso de mejora continua respecto de la protección de sus sistemas de Tecnologías de la Información y las Comunicaciones basados en una vigilancia permanente

de su exposición a las amenazas. Estos agentes deben servir como modelo de buenas prácticas en la gestión de la ciberseguridad.

En aplicación del principio de responsabilidad compartida, el sector público debe mantener estrechas relaciones con las empresas que gestionan los Sistemas de Tecnologías de la Información y las Comunicaciones relevantes para los intereses nacionales, intercambiando el conocimiento que permita una adecuada coordinación entre ambos y una cooperación efectiva que genere una sinergia apropiada dentro del entorno de la ciberseguridad.

El fortalecimiento de la ciberseguridad requiere un conocimiento sistemático sobre el impacto de una potencial interrupción o destrucción de las redes y sistemas que proporcionan servicios esenciales, así como métricas del nivel de seguridad de estos sistemas que permitan la oportuna toma de decisiones según su grado de exposición.

Objetivo II

Uso seguro y fiable del ciberespacio frente a su uso ilícito o malicioso

El ciberespacio juega un papel cada vez más importante tanto en la comisión de hechos ilícitos o maliciosos como en su investigación para promover la confianza de los ciudadanos. Es necesario garantizar una adecuada persecución de los fenómenos criminales que en él se desarrollen.

Son tres los ámbitos en los que se desenvuelve la lucha contra la cibercriminalidad: (i) el ciberespacio como objetivo directo de los hechos delictivos, o de la amenaza; (ii) el ciberespacio como medio clave para su comisión; y (iii) el ciberespacio como medio u objeto directo de investigación de cualquier tipo de hecho ilícito.

Sobre la base de una regulación sólida y eficaz que refuerce y garantice la lucha contra la cibercriminalidad, es necesario el fortalecimiento de la cooperación judicial y policial, tanto nacional como internacional, así como la asignación de recursos suficientes a los órganos competentes en la materia y la capacitación de los profesionales que trabajan en este ámbito.

Del mismo modo, es fundamental fomentar la colaboración y participación ciudadana, facilitando los procedimientos de acceso y transmisión de la información de interés judicial y policial e identificando aspectos que requieran de una mejora en las capacidades de las instituciones policiales y de los organismos judiciales competentes.

Objetivo III

Protección del ecosistema empresarial y social y de los ciudadanos

Todas las personas y organizaciones tienen derecho a hacer un uso seguro del ciberespacio. Es por ello responsabilidad del Estado promover e impulsar las medidas para alcanzar y mantener un nivel suficiente de ciberseguridad, que proteja especialmente a los más vulnerables y que permita el adecuado desarrollo socioeconómico de España.

La ciberseguridad es una responsabilidad compartida con los actores privados que, por acción u omisión, puedan afectarla; y no es posible conseguirla sin su participación. Por tanto, entre las medidas a impulsar deben estar aquellas que conduzcan a la necesaria cooperación para la seguridad común.

La defensa de ciudadanos, autónomos y empresas debe ir más allá de las medidas de autoprotección que ellos puedan tomar, por lo que es conveniente implantar medidas para su ciberdefensa activa. A la vez todos los usuarios del ciberespacio deben hacer un uso responsable de la tecnología a su alcance.

La acelerada adopción por la sociedad de tecnologías emergentes provoca que los riesgos evolucionen. Por ello, el intercambio permanente de conocimiento con los diferentes actores y el establecimiento de mecanismos de monitorización para la protección del ecosistema empresarial y social serán instrumentos que permitirán al Gobierno estar informado y tomar las decisiones oportunas para actualizar y adecuar las acciones resultado de la presente estrategia.

Objetivo IV

Cultura y compromiso con la ciberseguridad y potenciación de las capacidades humanas y tecnológicas

Para afrontar los desafíos que plantea la ciberseguridad, España debe contar con recursos técnicos y humanos que le proporcionen la autonomía tecnológica necesaria y la capacitación adecuada para el uso seguro del ciberespacio, situando a la ciberseguridad como habilitador clave para una nación emprendedora.

Para ello, debe mejorar la ciberseguridad colectiva difundiendo la cultura de la ciberseguridad con la ayuda de organismos públicos y privados y medios de comunicación, potenciando mecanismos de información y asistencia a los ciudadanos y fomentando espacios de encuentro entre la sociedad civil, administraciones y empresas.

Se debe también contribuir al uso seguro y responsable de las Tecnologías de la Información y de las Comunicaciones promoviendo la capacitación en ciberseguridad de los profesionales adecuada a la demanda del mercado laboral, estimulando el desarrollo de los profesionales con habilidades propias, impulsando la formación y cualificación especializada, así como las capacidades de generación de conocimiento, el desarrollo actividades de I+D+i en ciberseguridad y el fomento del uso de productos y servicios certificados.

Asimismo, merece especial atención la protección del patrimonio tecnológico y de la propiedad industrial e intelectual. Para promover la soberanía tecnológica y aprovechar las oportunidades que ofrece la transformación digital, se fomentará e impulsará la industria española de ciberseguridad y las mejores prácticas en el desarrollo e implantación de sistemas de información y comunicaciones.

Objetivo V

Seguridad del ciberespacio en el ámbito internacional

España promoverá un ciberespacio abierto, plural, seguro y confiable tanto en sus relaciones bilaterales como en las organizaciones multilaterales, regionales e internacionales, y en los foros y conferencias, donde la ciberseguridad ocupa un lugar destacado.

Abogará por la creación de un marco internacional para la prevención de conflictos, la cooperación y la estabilidad en el ciberespacio, en el que se apliquen los principios de La Carta de Naciones Unidas en su totalidad, el Derecho Internacional, los Derechos Humanos y el Derecho Humanitario Bélico, así como las normas no vinculantes sobre el comportamiento responsable de los Estados.

Consciente de la importancia del multilateralismo, considera relevante el papel de Naciones Unidas para avanzar en la construcción de consensos que, junto a la adopción y puesta en marcha de medidas de fomento de la confianza, la colaboración y participación de todos los actores implicados (Estados, sector privado, sociedad civil, usuarios y academia), constituyen la base para lograr seguridad y estabilidad en el ciberespacio y avanzar hacia su regulación.

En línea con nuestros socios europeos, reforzará la confianza en Internet, en la transformación digital y en el desarrollo de las nuevas tecnologías, contribuyendo a consolidar un ecosistema cibernético europeo seguro que permita avances hacia el mercado único digital. Para ello defenderá un internet interoperativo, neutral, abierto y diverso, reflejo de la pluralidad cultural y lingüística internacional, basado en un sistema de gobernanza democrático, representativo e inclusivo, resultado de la concertación y el consenso. Además, un acceso a internet global y generalizado, contribuyendo con ello al cumplimiento de los Objetivos de Desarrollo Sostenible.

Del mismo modo, nuestra pertenencia a la Unión Europea (UE), nos obliga a fortalecer la seguridad y la autonomía estratégica europea mediante la búsqueda de sinergias, la cooperación técnica, operativa, estratégica y política; a reforzar nuestra resiliencia, nuestra capacidad de respuesta ante las crisis y las complementariedades entre los ámbitos civiles y militares como socios de la UE y aliados de la Organización del Tratado del Atlántico Norte (OTAN).

Sobre la base de lo anterior, España continuará participando activamente en la UE y la OTAN; en Naciones Unidas, y en sus foros derivados como el Foro de Gobernanza de Internet (IGF); en la Organización para la Seguridad y la Cooperación en Europa (OSCE), en el desarrollo e implementación de las Medidas de Fomento de la Confianza; en la Organización de Estados Americanos (OEA). Así como con el Foro Global del Expertos en Ciberseguridad (GFCE) y la Coalición por la Libertad en Internet (Freedom Online Coalition. FOC), sin olvidar nuestra presencia en el Centro Europeo de Excelencia para contrarrestar las Amenazas Híbridas (Hybrid CoE), así como en el Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN (CCD CoE).

Además, reforzará la cooperación internacional bilateral en materia de ciberseguridad, promoverá relaciones fluidas y de confianza en este ámbito, colaborará en la construcción de capacidades en terceros Estados, prestando especial atención a las mujeres y los jóvenes y fomentará la creación de canales de información e intercambio de experiencias, impulsando, para todo ello, la adopción de acuerdos bilaterales y multilaterales en este ámbito.

CAPÍTULO 4

Líneas de acción y medidas

En este capítulo se establecen las líneas de acción dirigidas a la consecución de los objetivos establecidos.

Línea de Acción 1. Reforzar las capacidades ante las amenazas provenientes del ciberespacio:

Esta línea de acción responde al Objetivo I de la Estrategia.

Medidas:

1. Ampliar y mejorar las capacidades de detección y análisis de las ciberamenazas de manera que se permita la identificación de procedimientos y orígenes de ataque, así como la elaboración de la inteligencia necesaria para una protección, atribución y defensa más eficaz.
2. Potenciar la colaboración de los centros de excelencia e investigación en la lucha contra las ciberamenazas.
3. Potenciar la creación, difusión y aplicación de mejores prácticas, y la adopción de estándares en materia de ciberseguridad.
4. Asegurar la coordinación técnica y operacional de los organismos con responsabilidades en ciberseguridad, las empresas y la sociedad.
5. Desarrollar y mantener actualizadas las normas, procedimientos e instrucciones de respuesta frente a incidentes de ciberseguridad, asegurando su integración en el Sistema de Seguridad Nacional.
6. Potenciar las capacidades de ciberdefensa y de ciberinteligencia.
7. Promover la participación de las empresas en plataformas sectoriales para el intercambio y análisis de información, así como para la medida del riesgo sectorial y la propuesta de acciones que lo mitiguen, acompañadas de requerimientos legales que las regulen.
8. Potenciar y apoyar los desarrollos realizados en la red de CSIRT española.
9. Impulsar el desarrollo de plataformas de notificación, intercambio de información y coordinación para la mejora de la ciberseguridad sectorial.
10. Desarrollar instrumentos de prevención, detección, respuesta, retorno a la normalidad y evaluación enfocados a la gestión de crisis para el ámbito de la ciberseguridad en el marco de la Seguridad Nacional.
11. Garantizar la coordinación, la cooperación y el intercambio de información sobre ciberincidentes e inteligencia de ciberamenazas entre el sector público, el sector privado y los organismos internacionales competentes, fomentando la prevención y la alerta temprana.
12. Implantar medidas de ciberdefensa activa en el sector público con el objetivo de mejorar las capacidades de respuesta.

Línea de Acción 2. Garantizar la seguridad y resiliencia de los activos estratégicos para España:

Esta línea de acción responde al Objetivo I de la Estrategia.
Medidas:

1. Ampliar y fortalecer las capacidades de prevención, detección, respuesta, recuperación y resiliencia a los ciberataques dirigidos al sector público, a los servicios esenciales y a empresas de interés estratégico.
2. Potenciar el desarrollo de la normativa sobre protección de infraestructuras críticas, reforzando la seguridad de las redes y sistemas de información que las soportan.
3. Asegurar la plena implantación del Esquema Nacional de Seguridad, del Sistema de Protección de las Infraestructuras Críticas, y el cumplimiento y armonización de la normativa sobre protección de infraestructuras críticas y servicios esenciales, con un enfoque prioritario basado en el riesgo.
4. Potenciar, en el marco de sus competencias, la progresiva implicación y creación de infraestructuras de ciberseguridad en las Comunidades Autónomas, las Ciudades Autónomas, las Entidades Locales y en sus organismos vinculados o dependientes que cooperarán y se coordinarán con las estructuras nacionales en pro de la mejora de la ciberseguridad nacional.
5. Desarrollar el Centro de Operaciones de Ciberseguridad de la Administración General del Estado que mejore las capacidades de prevención, detección y respuesta, e impulsar el desarrollo de centros de operaciones de ciberseguridad en el ámbito autonómico y local.
6. Reforzar la implantación de infraestructuras y servicios de telecomunicaciones y sistemas de información horizontales comunes, y compartidos por las Administraciones Públicas, potenciando su uso y sus capacidades de seguridad y resiliencia, asegurando a la par, la coordinación con los primeros en aquellos casos que no se utilicen las infraestructuras y servicios comunes.
7. Impulsar el desarrollo de un sistema de métricas de las principales variables de ciberseguridad que permita a las autoridades competentes determinar el nivel de seguridad y su evolución.
8. Comprometer al sector público y al privado en la gestión de los riesgos de la cadena de suministro, especialmente en aquellos que afecte a la provisión de servicios esenciales.
9. Desarrollar catálogos de productos y servicios cualificados y certificados, para su empleo en los procesos de contratación del sector público y de los servicios esenciales.
10. Reforzar las estructuras de seguridad y la capacidad de vigilancia de los sistemas de información que manejan información clasificada.
11. Promover la realización de ciberejercicios y evaluaciones de ciberseguridad, especialmente en áreas que puedan afectar a la Seguridad Nacional, la Administración pública, los servicios esenciales y las empresas cotizadas.
12. Asegurar la protección de las Infraestructuras Científico-Técnicas Singulares y los centros de referencia de I+D+i.

Línea de Acción 3. Reforzar las capacidades de investigación y persecución de la cibercriminalidad, para garantizar la seguridad ciudadana y la protección de los derechos y libertades en el ciberespacio:

Esta línea de acción responde al Objetivo II de la Estrategia.
Medidas:

1. Reforzar el marco jurídico para responder eficazmente a la cibercriminalidad, tanto en lo relativo a la definición de tipos penales como en la regulación de adecuadas medidas de investigación.
2. Fomentar la colaboración y participación ciudadana, articulando instrumentos de intercambio y transmisión de información de interés policial, y promoviendo el desarrollo de campañas de prevención de la cibercriminalidad orientadas a ciudadanos y empresas.
3. Reforzar las acciones encaminadas a potenciar las capacidades de investigación, atribución, persecución y, en su caso, la actuación penal, frente a la cibercriminalidad.
4. Fomentar el traslado a los organismos competentes de la jurisdicción penal de la información relativa a incidentes de seguridad que presenten caracteres de delito, y especialmente de aquellos que afecten o puedan afectar a la provisión de los servicios esenciales y a las infraestructuras críticas.

5. Procurar a los operadores jurídicos el acceso a información y recursos materiales que aseguren una mejor aplicación del marco jurídico y técnico relacionado con la lucha contra la cibercriminalidad, y que les dote de mayores capacidades para la investigación y enjuiciamiento de los hechos ilícitos que correspondan.

6. Fomentar el intercambio de información, experiencia y conocimientos, entre el personal con responsabilidades en la investigación y persecución de la cibercriminalidad.

7. Asegurar a los profesionales del Derecho y a las Fuerzas y Cuerpos de Seguridad del Estado el acceso a los recursos humanos y materiales que les proporcionen el nivel necesario de conocimientos para la mejor aplicación del marco legal y técnico asociado.

8. Impulsar la coordinación de las investigaciones sobre cibercriminalidad y otros usos ilícitos del ciberespacio entre los distintos órganos y unidades con competencia en esta materia.

9. Fortalecer la cooperación judicial y policial internacional.

Línea de Acción 4. Impulsar la ciberseguridad de ciudadanos y empresas:

Esta línea de acción responde al Objetivo III de la Estrategia.

Medidas:

1. Ofrecer a los ciudadanos y al sector privado un servicio público de ciberseguridad integrado, de calidad y de fácil acceso, y que sea un estímulo a la demanda de los servicios que ofrece el sector empresarial de la ciberseguridad.

2. Impulsar la ciberseguridad en las pymes, micropymes y autónomos mediante la articulación de políticas públicas en ciberseguridad, y especialmente con actuaciones dirigidas al fomento de la resiliencia.

3. Promover la ciberseguridad para garantizar la privacidad y protección de datos personales dentro del marco de los derechos digitales del ciudadano acorde con el ordenamiento jurídico, promoviendo la protección de la «identidad digital».

4. Crear mecanismos ágiles y seguros de denuncia para el sector privado y ciudadanos.

5. Estimular la cooperación entre actores públicos y privados, en particular promoviendo el compromiso de los Proveedores de Servicios de Internet y de Servicios Digitales para mejorar la ciberseguridad. Se impulsará la regulación nacional en este sentido y se implantarán medidas de ciberdefensa activa de ciudadanos y pymes.

6. Desarrollar mecanismos para la medida agregada del riesgo y su evolución, tanto de ciudadanos como de empresas, para priorizar medidas de ciberseguridad e informar adecuadamente a la sociedad.

7. Impulsar en el sector empresarial la implantación de estándares reconocidos de ciberseguridad. Estimular, junto con las entidades de normalización nacional e internacional, la creación, difusión y aplicación de mejores prácticas sectoriales en materia de ciberseguridad, incluidos diferentes esquemas de certificación.

8. Impulsar la implantación de sistemas fiables de identificación electrónica y servicios electrónicos de confianza.

9. Promover la creación del foro Nacional de Ciberseguridad, que integre a representantes de la sociedad civil, expertos independientes, sector privado, la academia, asociaciones, organismos sin ánimo de lucro, entre otros, con el objetivo de potenciar y crear sinergias público privadas, particularmente en la generación de conocimiento sobre las oportunidades y amenazas para la seguridad en el ciberespacio.

Línea de Acción 5. Potenciar la industria española de ciberseguridad, y la generación y retención de talento, para el fortalecimiento de la autonomía digital:

Esta línea de acción responde al Objetivo IV de la Estrategia.

Medidas:

1. Impulsar programas de apoyo a la I+D+i en seguridad digital y ciberseguridad en pymes, empresas, universidades y centros de investigación, facilitando el acceso a programas de incentivos nacionales e internacionales y mediante programas de compra pública innovadora.

2. Dinamizar el sector industrial y de servicios de ciberseguridad, incentivando medidas de apoyo a la innovación, a la inversión, a la internacionalización y a la transferencia tecnológica en especial en el caso de micropymes y pymes.

3. Incrementar las actividades nacionales para el desarrollo de productos, servicios y sistemas de ciberseguridad, y la seguridad desde el diseño, apoyando específicamente aquellas que sustenten necesidades de interés nacional para fortalecer la autonomía digital, y la propiedad intelectual e industrial.

4. Promover las actividades de normalización y la exigencia de requisitos ciberseguridad en los productos y servicios de Tecnologías de la Información y de las Comunicaciones, facilitar el acceso a productos y servicios que respondan a estos requisitos, promoviendo la evaluación de la conformidad y la certificación, y apoyando la elaboración de catálogos.

5. Actualizar, o en su caso desarrollar marcos de competencias en ciberseguridad, que respondan a las necesidades del mercado laboral.

6. Identificar las necesidades de capacidades profesionales de ciberseguridad, fomentando la colaboración con las instituciones educativas y formativas impulsando la formación continua, la formación para el empleo y universitaria, promoviendo sistemas de acreditación y certificación profesional.

7. Impulsar la inclusión de perfiles profesionales de ciberseguridad en las relaciones de puestos de trabajo del sector público.

8. Detectar, fomentar y retener el talento en ciberseguridad, con especial atención al campo de la investigación.

9. Impulsar programas específicos de I+D+i en ciberseguridad y ciberdefensa.

Línea de Acción 6. Contribuir a la seguridad del ciberespacio en el ámbito internacional, promoviendo un ciberespacio abierto, plural, seguro y confiable, en apoyo de los intereses nacionales:

Esta línea de acción responde al Objetivo V de la Estrategia.

Medidas:

1. Potenciar y reforzar la presencia de España en las organizaciones, conferencias y foros regionales e internacionales y a los que pertenece y en los que la ciberseguridad forma parte sustancial de sus agendas, y apoyar y participar de manera activa en las diferentes iniciativas, coordinando la posición de los diferentes agentes nacionales implicados.

2. Promover en el ámbito de Naciones Unidas la búsqueda de consensos para el pleno respeto a la Carta de Naciones Unidas y la aplicación y puesta en práctica del Derecho Internacional y las normas para el comportamiento responsable de los Estados. Y del mismo modo avanzar en la adopción e implementación de Medidas para el Fomento de la Confianza en el ciberespacio.

3. Participar activamente en la Unión Europea en el desarrollo de un ecosistema europeo seguro que favorezca el avance y la consolidación del mercado único, y la seguridad y autonomía estratégica de Europa, buscando las complementariedades y la cooperación entre la Unión Europea y la OTAN.

4. Fomentar el diálogo bilateral, la cooperación y los sistemas de intercambio de información, alerta temprana y de experiencias para desarrollar un enfoque coordinado en la lucha contra las ciberamenazas con otros países, promoviendo la negociación y firma de acuerdos internacionales.

5. Promover el desarrollo de capacidades tecnológicas y el acceso a internet en terceros países para contribuir con ello al cumplimiento de los Objetivos de Desarrollo Sostenible.

6. Desarrollar con los países de nuestro entorno una mayor conciencia sobre las Amenazas Híbridas, limitando su impacto sobre la soberanía e integridad de nuestros países.

Línea de Acción 7. Desarrollar una cultura de ciberseguridad:

Las medidas incluidas en esta Línea de Acción contribuirán al Plan de Cultura de Seguridad Nacional y responde al objetivo IV de la Estrategia.

Medidas:

1. Incrementar las campañas de concienciación a ciudadanos y empresas, y poner a su disposición información útil adaptada a cada perfil, especialmente en el ámbito de los autónomos, pequeñas y medianas empresas.

2. Potenciar actuaciones encaminadas al incremento de la corresponsabilidad y obligaciones de la sociedad en la ciberseguridad nacional.

3. Impulsar iniciativas y planes de alfabetización digital en ciberseguridad.
4. Promover la difusión de la cultura de la ciberseguridad como una buena práctica empresarial, y reconocer la implicación de las empresas en la mejora de la ciberseguridad colectiva como responsabilidad social corporativa.
5. Promover un espíritu crítico en favor de una información veraz y de calidad y que contribuya a la identificación de las noticias falsas y la desinformación.
6. Concienciar a directivos de organizaciones, a los efectos de que habiliten los recursos necesarios y promuevan los proyectos de ciberseguridad que sus entidades puedan necesitar.
7. Promover la concienciación y formación en ciberseguridad en los centros de enseñanza, adaptada a todos los niveles formativos y especialidades.
8. Buscar y reconocer la colaboración y participación de medios de comunicación, para lograr un mayor alcance en las campañas dirigidas a ciudadanos y, en especial, a menores de edad.

CAPÍTULO 5

La ciberseguridad en el Sistema de Seguridad Nacional

En este capítulo se contempla la integración de la ciberseguridad en el actual Sistema de Seguridad Nacional.

La Estrategia de Ciberseguridad Nacional de 2013 y la posterior aprobación de la Ley de Seguridad Nacional de 2015 establecen una estructura orgánica específica para la ciberseguridad. En la presente Estrategia de 2019 se impulsan iniciativas que complementan los nuevos avances en el modelo de gobernanza nacional con las políticas europeas.

La estructura de la ciberseguridad en el marco del Sistema de Seguridad Nacional está constituida por los siguientes componentes:

1. El Consejo de Seguridad Nacional.
2. El Comité de Situación, único para el conjunto del Sistema de Seguridad Nacional ante situaciones de crisis.
3. El Consejo Nacional de Ciberseguridad.
4. La Comisión Permanente de Ciberseguridad.
5. El Foro Nacional de Ciberseguridad.
6. Las Autoridades públicas competentes y los CSIRT de referencia nacionales.

El Consejo de Seguridad Nacional:

El Consejo de Seguridad Nacional, en su condición de Comisión Delegada del Gobierno para la Seguridad Nacional, es el órgano al que corresponde asistir al Presidente del Gobierno en la dirección de la Política de Seguridad Nacional.

El Consejo de Seguridad Nacional actúa, a través del Departamento de Seguridad Nacional como punto de contacto único para ejercer una función de enlace y garantizar la cooperación transfronteriza con otros países de la Unión Europea.

El Comité de Situación:

El Comité de Situación tiene carácter único para el conjunto del Sistema de Seguridad Nacional y actuará, apoyado por el Departamento de Seguridad Nacional, de acuerdo con las directrices político-estratégicas dictadas por el Consejo de Seguridad Nacional en materia de gestión de crisis.

El Consejo Nacional de Ciberseguridad:

El Consejo Nacional de Ciberseguridad da apoyo al Consejo de Seguridad Nacional para el cumplimiento de sus funciones y, en particular, en la asistencia al Presidente del Gobierno en la dirección y coordinación de la Política de Seguridad Nacional en el ámbito de la ciberseguridad.

Entre sus funciones se encuentran reforzar las relaciones de coordinación, colaboración y cooperación entre las distintas Administraciones Públicas con competencias en materia de ciberseguridad, así como entre los sectores público y privado, y facilitar la toma de decisiones del propio Consejo mediante el análisis, estudio y propuesta de iniciativas tanto

en el ámbito nacional como en el internacional, así como realizar la valoración de los riesgos y amenazas, analizar los posibles escenarios de crisis, estudiar su posible evolución, elaborar y mantener actualizados los planes de respuesta y formular directrices para la realización de ejercicios de gestión de crisis en el ámbito de la ciberseguridad y evaluar los resultados de su ejecución, todo ello en coordinación con los órganos y autoridades directamente competentes.

La Comisión Permanente de Ciberseguridad:

La Comisión Permanente de Ciberseguridad se establece con objeto de facilitar la coordinación interministerial a nivel operacional en el ámbito de la ciberseguridad. Presidida por el Departamento de Seguridad Nacional, se compone de aquellos órganos y organismos representados en el Consejo Nacional de Ciberseguridad con responsabilidades operativas. Es el órgano al que corresponde asistir al Consejo Nacional de Ciberseguridad sobre aspectos relativos a la valoración técnica y operativa de los riesgos y amenazas a la ciberseguridad.

El funcionamiento de la Comisión se enmarca en el procedimiento de gestión de crisis en el ámbito de la ciberseguridad. Dicho procedimiento establece sus funciones dirigidas a detectar y valorar los riesgos y amenazas; facilitar el proceso de toma de decisiones y asegurar una respuesta óptima y coordinada de los recursos del Estado. Además, incluye los diferentes niveles de activación del Sistema de Seguridad Nacional, e instrucciones para la gestión de la comunicación pública.

A fin de responder de manera oportuna y proporcionada a situaciones de especial relevancia en el desarrollo de sus funciones, se progresará en la definición de sus capacidades y responsabilidades.

Foro Nacional de Ciberseguridad:

Actuará en la potenciación y creación de sinergias público privadas, particularmente en la generación de conocimiento sobre las oportunidades y los desafíos y amenazas a la seguridad en el ciberespacio.

La puesta en marcha del foro Nacional de Ciberseguridad, y la armonización de su funcionamiento con los órganos existentes, se realizará mediante la aprobación de las disposiciones normativas necesarias, con el objetivo de alcanzar el funcionamiento coordinado y eficiente de estos componentes en el Sistema de Seguridad Nacional.

Autoridades públicas competentes y los CSIRT de referencia nacionales:

El marco estratégico e institucional de la ciberseguridad se complementa con las autoridades públicas competentes en materia de seguridad de las redes y sistemas de información y los CSIRT de referencia nacional que se recogen en el marco jurídico nacional.

Asimismo, los CSIRT de las Comunidades Autónomas, de las Ciudades Autónomas, de las Entidades Locales y sus organismos vinculados o dependientes, los de las entidades privadas, la red de CSIRT.es y otros servicios de ciberseguridad relevantes deberán estar coordinados con los anteriores en función de las competencias de cada uno de ellos. De igual modo, desde los CSIRT nacionales, en colaboración con los CSIRT autonómicos y privados, se fomentará la puesta en marcha de iniciativas que contribuyan a la consecución de los objetivos de la estrategia nacional.

Consideraciones finales y evaluación:

La experiencia adquirida desde la Estrategia de Ciberseguridad Nacional de 2013, ha permitido plasmar en el presente documento una actualización de las amenazas y los desafíos a las que nos enfrentamos, siempre en continua evolución. Para adecuarse a este nuevo escenario cambiante, se proponen un conjunto de Líneas de Acción y medidas más dinámicas que permitan, si fuese necesario, una rápida adaptación del ecosistema de ciberseguridad nacional, basadas en un modelo de gobernanza con una considerable madurez, donde debe participar activamente el sector privado y el resto de la sociedad civil.

En este sentido, la Estrategia se concibe como un documento vivo que ha de adaptarse a la evolución de la ciberseguridad, por lo que deberá ser objeto de revisión continua, como también los planes específicos y sectoriales que de ella se deriven. Se elaborará un informe

anual de evaluación de la Estrategia donde figurará el grado de ejecución y cumplimiento de sus objetivos.

Por otro lado, a la vista del incremento de las amenazas y desafíos a la ciberseguridad y cómo los afrontan países de nuestro entorno, resulta cada vez más urgente dotarse de recursos económicos, humanos y materiales para hacer frente a los mismos. Una de las acciones especialmente relevantes en este marco es que el Centro de Operaciones de Ciberseguridad de la Administración General del Estado se encuentre adecuadamente dotado.

§ 20

Real Decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021

Presidencia del Gobierno
«BOE» núm. 314, de 31 de diciembre de 2021
Última modificación: sin modificaciones
Referencia: BOE-A-2021-21884

La Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, establece que la política de Seguridad Nacional es una política pública, en la que bajo la dirección del Presidente del Gobierno y la responsabilidad del Gobierno, participan todas las administraciones públicas, de acuerdo con sus respectivas competencias, y la sociedad en general, para responder a las necesidades de la Seguridad Nacional.

Para materializar esta visión inclusiva del conjunto de los componentes del sector público, del sector privado y de la sociedad en su conjunto en la plasmación de la política de Seguridad Nacional, la citada ley prevé que la Estrategia de Seguridad Nacional se configure como el marco político estratégico de referencia de la Política de Seguridad Nacional. Asimismo, prevé que contendrá el análisis del entorno estratégico, la concreción de los riesgos y amenazas que afectan a la seguridad de España, la definición de las líneas de acción estratégicas en cada ámbito de actuación y la promoción de la optimización de los recursos existentes.

A nivel procedimental, establece que será elaborada a iniciativa del Presidente del Gobierno, quien la someterá a la aprobación del Consejo de Ministros, y se revisará cada cinco años o cuando lo aconsejen las circunstancias cambiantes del entorno estratégico. Una vez aprobada, será presentada en las Cortes Generales y, en concreto, en la Comisión Mixta Congreso-Senado de Seguridad Nacional.

En el año 2011 se aprobó la primera Estrategia Española de Seguridad al término de la IX Legislatura, sin margen temporal para su desarrollo.

En la X Legislatura, y tras la adecuación de la estructura de la Presidencia del Gobierno que dio carta de naturaleza a la creación del Departamento de Seguridad Nacional, por Real Decreto 1119/2012, de 20 de julio, se procedió a la revisión de la Estrategia de 2011, que tras un proceso de amplio espectro, consensuado a nivel político y abierto a la sociedad, cristalizó el 31 de mayo de 2013 en una nueva Estrategia de Seguridad Nacional, estrategia que fue sustituida por la aprobada a propuesta del Presidente del Gobierno y previa deliberación del Consejo de Ministros en su reunión del día 1 de diciembre de 2017, vigente actualmente.

El Presidente del Gobierno consideró que las circunstancias cambiantes, planteadas en España y en el mundo en general por la situación de la pandemia de la COVID-19 hacían necesario adelantar el periodo de renovación de la Estrategia de Seguridad Nacional vigente desde el año 2017 y, en la reunión del Consejo de Seguridad Nacional del 22 de junio de 2020, dio el mandato de iniciar la elaboración de una nueva estrategia, ahora materializada.

A iniciativa del Presidente del Gobierno, el Consejo de Seguridad Nacional celebrado el día 6 de octubre de 2020 adoptó el Acuerdo por el que se aprueba el procedimiento para la elaboración de la Estrategia de Seguridad Nacional 2021, y que ha sido elaborada de acuerdo con las previsiones de la Ley de Seguridad Nacional.

Las motivaciones que han impulsado la revisión de la vigente Estrategia se centran en la necesidad de adaptarla a la cambiante situación de los ámbitos de la Seguridad Nacional, sin olvidar el importante cambio operado por la pandemia de la COVID-19, que obligan a todos los poderes públicos a profundizar en la forma de garantizar los derechos y el bienestar de los ciudadanos, garantizando la defensa de España y sus principios y valores constitucionales.

El texto de la nueva Estrategia, elaborado de conformidad con el procedimiento aprobado en el acuerdo antes mencionado, ha sido sometido a informe favorable del Consejo de Seguridad Nacional en su reunión celebrada el día 18 de noviembre de 2021.

La aprobación de la Estrategia corresponde al Gobierno mediante real decreto según dispone el artículo 14.b) de la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, a propuesta del Presidente del Gobierno, según lo establecido en el artículo 15.b) del mismo texto legal.

En su virtud, a propuesta del Presidente del Gobierno, y previa deliberación del Consejo de Ministros en su reunión del día 28 de diciembre de 2021,

DISPONGO:

Artículo único. *Aprobación de la Estrategia de Seguridad Nacional 2021.*

Se aprueba la Estrategia de Seguridad Nacional 2021, la cual se configura como el marco político-estratégico de referencia de la política de Seguridad Nacional, y cuyo texto se incluye a continuación.

Disposición derogatoria única. *Derogación normativa.*

Queda derogado el Real Decreto 1008/2017, de 1 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2017.

Disposición final primera. *Títulos competenciales.*

Este real decreto se dicta al amparo de los títulos competenciales previstos en el artículo 149.1.4.ª y 29.ª de la Constitución Española, que atribuye al Estado la competencia exclusiva en materia de Defensa y Fuerzas Armadas y en materia de seguridad pública, respectivamente.

Disposición final segunda. *Habilitación para el desarrollo reglamentario.*

Se autoriza al Gobierno para dictar cuantas disposiciones sean necesarias para el desarrollo de este real decreto.

Disposición final tercera. *Entrada en vigor.*

El presente real decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

ESTRATEGIA DE SEGURIDAD NACIONAL 2021

El Consejo de Seguridad Nacional ha sido el órgano responsable de la elaboración de la Estrategia de Seguridad Nacional 2021, en cuyo proceso han participado los departamentos ministeriales y el Centro Nacional de Inteligencia.

También han participado las Comunidades y Ciudades Autónomas a través de la Conferencia Sectorial para Asuntos de Seguridad Nacional.

La Estrategia de Seguridad Nacional 2021 incluye asimismo las aportaciones de expertos independientes, personas de reconocido prestigio, conocimientos y experiencia en el campo de la seguridad.

La coordinación del proceso ha sido llevada a cabo por el Departamento de Seguridad Nacional del Gabinete de la Presidencia del Gobierno en su condición de Secretaría Técnica y Órgano de Trabajo Permanente del Consejo de Seguridad Nacional.

RESUMEN EJECUTIVO

La Estrategia de Seguridad Nacional 2021 se estructura en cinco capítulos.

El primer capítulo, titulado «Seguridad Global y Vectores de Transformación», analiza el contexto internacional de seguridad. La Estrategia identifica la pandemia de la COVID-19 como un factor que ha producido una aceleración de las principales dinámicas globales que afectan a la seguridad. Sin poder afirmar categóricamente que se trata de un cambio de era, sí que se percibe el momento actual como etapa de transición. La característica predominante es la incertidumbre sobre un futuro donde la transformación digital y la transición ecológica se configuran como las principales palancas de cambio en un escenario de mayor competición geopolítica.

El segundo capítulo, «Una España Segura y Resiliente», traza un perfil de España y su seguridad. Desde su identificación como país de condición europea, mediterránea y atlántica, se realiza un recorrido geográfico, donde Europa, Magreb y Oriente Próximo, África Subsahariana, América del Norte, América Latina y el Caribe, y Asia-Pacífico se analizan desde el prisma de la Seguridad Nacional.

El tercer capítulo recoge los riesgos y las amenazas a la Seguridad Nacional, cuyas principales características son su interrelación y dinamismo. De esta forma, el seguimiento de las conexiones entre riesgos resulta tan importante como su análisis de forma independiente. La principal actualización en el mapa de riesgos es la inclusión de las campañas de desinformación. Además, la tecnología y las estrategias híbridas son elementos transversales al conjunto de riesgos y amenazas a la Seguridad Nacional.

El cuarto capítulo, titulado «Un Planeamiento Estratégico Integrado», establece tres objetivos, que marcan las prioridades de la Seguridad Nacional para este ciclo estratégico. El primer objetivo es avanzar en materia de gestión de crisis; el segundo objetivo es favorecer la dimensión de la seguridad de las capacidades tecnológicas y los sectores estratégicos; y el tercer objetivo es desarrollar la capacidad preventiva, de detección y respuesta frente a las estrategias híbridas.

A continuación, la Estrategia traza tres ejes –proteger, promover y participar– sobre los que se estructuran las líneas de acción. Este planteamiento otorga especial relevancia al avance en la integración del Sistema de Seguridad Nacional y a la acción frente a situaciones de crisis. A los efectos de articular una política preventiva, se identifica como área clave el establecimiento de un sistema de alerta temprana, sobre una base tecnológica, que proporcione indicadores para todos los ámbitos de la Seguridad Nacional.

La Estrategia de Seguridad Nacional 2021 plantea iniciativas necesarias, como por ejemplo, la creación de una reserva estratégica basada en capacidades nacionales de producción industrial o el desarrollo de un plan integral de seguridad para Ceuta y Melilla.

En el plano internacional, España apuesta por una mayor autonomía estratégica europea, donde al impulso de la Política Común de Seguridad y Defensa y del espacio de libertad, seguridad y justicia se unen la mejora de la seguridad sanitaria, el avance en la unión energética o el mayor protagonismo de la Unión Europea en la gestión de crisis transfronterizas. Además, en materia de seguridad colectiva, la revisión estratégica de la OTAN supondrá un hito importante, que incluirá la colaboración con la Unión Europea como una de sus líneas de acción.

Finalmente, el quinto capítulo está dedicado a la gestión de crisis en el marco del Sistema de Seguridad Nacional, con un enfoque que parte de una visión del principio de resiliencia que incluye la progresión desde una situación de normalidad hasta la recuperación después de una situación de crisis. El avance en la integración del Sistema se materializa en actuaciones concretas. La primera de ellas es la elaboración de un catálogo de recursos de la Seguridad Nacional. La segunda es la preparación de planes de respuesta para determinados escenarios. La tercera es el desarrollo de un sistema de alerta temprana y análisis con indicadores que faciliten la toma de decisiones basada en datos objetivos concretos. La cuarta medida hace referencia a la integración de la información de la Seguridad Nacional a través de soluciones tecnológicas. La mejora de las comunicaciones

especiales de la Presidencia del Gobierno es la quinta medida, que contribuirá a la eficiencia del Sistema de Seguridad Nacional, al permitir una mayor coordinación entre administraciones en materia de gestión de crisis. La sexta y última medida contempla la integración de las Comunidades y Ciudades Autónomas en el Sistema de Seguridad Nacional.

INTRODUCCIÓN

En condiciones normales, la revisión de la Estrategia de Seguridad Nacional 2017 hubiese llevado a cabo pasados cinco años. Sin embargo, el impacto de la pandemia de la COVID-19 y el incremento en el empleo de estrategias híbridas han aconsejado una revisión estratégica que permita enfrentar los riesgos y las amenazas en un renovado contexto de globalización, condicionado por una mayor incertidumbre y un cambio acelerado.

La pandemia ha sido el evento con mayor impacto global desde la Segunda Guerra Mundial, con grave afectación a la salud, la economía y la seguridad. Aun cuando se hayan superado todos sus efectos, perdurará la interdependencia del mundo actual, que contribuye a generar vulnerabilidades y a menudo actúa como factor multiplicador de las amenazas a medio y a largo plazo. Las pandemias, el cambio climático, los ciberataques o las crisis financieras son todos riesgos y amenazas complejas, a menudo interconectadas, que pueden desencadenar crisis en cascada.

En particular, los efectos del cambio climático pueden agudizar crisis económicas, políticas y geopolíticas derivadas de la escasez alimentaria e hídrica en muchas partes del mundo. Como consecuencia, podrían agravarse las situaciones de migraciones masivas, inestabilidad regional e incluso producirse nuevos conflictos armados. Asimismo, el calentamiento global tendrá repercusiones directas en España, pues provocará fenómenos meteorológicos adversos más extremos y frecuentes, sequías, olas de calor, inundaciones, escasez de agua y perjuicios para la biodiversidad.

Por otra parte, como muestra la realidad de los últimos años, el uso de estrategias híbridas por parte de actores estatales y no estatales como herramienta para presionar a los gobiernos democráticos es cada vez más frecuente.

A la hora de responder a las amenazas globales se plantea un dilema entre el repliegue estratégico de los Estados como forma de protección y la necesaria colaboración e intercambio de información entre países y organizaciones para buscar soluciones conjuntas. Este dilema paradigmático dificulta la articulación de respuestas en el marco de las organizaciones internacionales.

Por eso, ante futuras amenazas y crisis globales, será importante invertir esfuerzos en reforzar un sistema multilateral universal y regional que sea capaz de responder de forma coordinada y efectiva. En este sentido, y a la luz de la experiencia en Afganistán, la Unión Europea debe efectuar acciones conjuntas militares que contribuyan a reforzar el vínculo trasatlántico y que favorezcan la gestión de crisis transfronterizas y su autonomía estratégica. En particular, la Unión Europea debe asumir un mayor papel a la hora de gestionar desafíos, como las pandemias, el terrorismo internacional, los ciberataques o las campañas de desinformación, que requieren respuestas colectivas y la integración de capacidades.

La magnitud de los riesgos y las amenazas actuales requiere la correcta adecuación de los recursos, medios, sistemas y organizaciones disponibles para hacerles frente. La pandemia ha puesto de relieve la importancia de los sistemas de alerta temprana, de la fusión y el análisis de la información y de los planes de respuesta para la gestión de crisis, medidas todas ellas que facilitan y agilizan la toma de decisiones. Para ello, es necesario disponer de un Sistema de Seguridad Nacional digitalizado, capaz de proporcionar datos para la toma de decisiones en tiempo oportuno.

La prevención y la adaptación serán las claves para lograr un Sistema de Seguridad Nacional eficiente. Esto requiere:

Más anticipación: La Estrategia de Seguridad Nacional debe orientar la implantación de un sistema de alerta temprana y la preparación de planes de gestión de crisis. Todo ello con la participación de las Comunidades Autónomas, ya que numerosos recursos y capacidades de detección y gestión están entre sus competencias transferidas.

Más integración: La visión integral de la Seguridad Nacional requiere la necesaria coordinación del conjunto de las Administraciones Públicas y recursos del Estado, la colaboración público-privada y la implicación de la ciudadanía.

Más resiliencia: Para reducir la vulnerabilidad es tan necesario mitigar riesgos como robustecer la resiliencia, es decir, la capacidad de resistencia, transformación y recuperación ante una situación adversa.

Además, para gestionar futuras crisis y poder contar con los recursos críticos necesarios, es importante asegurar que las cadenas de suministro de estos recursos no dependan excesivamente del exterior. Asimismo, esto contribuirá a contener la expansión de las crisis, al fortalecer la resiliencia de la sociedad y de la economía.

CAPÍTULO 1

Seguridad global y vectores de transformación

El primer capítulo de la Estrategia de Seguridad Nacional describe el contexto internacional de seguridad y traza las principales dinámicas de transformación.

El orden global y el paradigma socio-económico liberal se encuentran en un periodo de cambio, sin que aún se haya definido claramente el nuevo panorama del sistema internacional. Los principales vectores de transformación son: el contexto geopolítico, el entorno socio-económico, la transformación digital y la transición ecológica.

Contexto geopolítico

El escenario geopolítico global se encuentra en un punto de inflexión. Por un lado, la arquitectura del sistema internacional se ve sujeta a una mayor presión y se recrudecen las controversias entre Estados. Por otro, se reivindica la necesidad de un multilateralismo eficaz para hacer frente a crisis de carácter global.

Se observa tensión entre las políticas de corte proteccionista o unilateral y los esfuerzos, sobre todo de la Unión Europea, para fortalecer el multilateralismo.

En los últimos años, las dinámicas de confrontación y competencia han prevalecido sobre las de negociación y acuerdo, lo que se ha traducido en un deterioro generalizado de las relaciones internacionales en todas sus facetas: comercial, tecnológica, diplomática o militar. Además, el declive democrático experimentado durante los últimos años contribuye a una mayor inestabilidad y dificulta la adopción de soluciones conjuntas.

En consecuencia, en muchas ocasiones, la gobernanza internacional en aspectos de seguridad, cambio climático o bienes públicos globales se ha visto suplantada por una cooperación ad hoc, marcada por alianzas de geometría variable. Esta tendencia se ha visto favorecida por los cambios en la distribución de poder y está contribuyendo a un multilateralismo de nuevo cuño, híbrido y con más actores emergentes y no estatales.

A su vez, ha aumentado el uso de las estrategias híbridas que, mediante acciones coordinadas y multidimensionales, tratan de explotar las vulnerabilidades de los Estados y sus instituciones con un objetivo de desestabilización o coerción política, social o económica. Estas estrategias se caracterizan por la dificultad de atribuir su autoría y por emplear medios que pueden incluir, además de acciones convencionales, otras como campañas de desinformación, ciberataques, espionaje, subversión social, sabotaje, coacción económica o el uso asimétrico de medios militares.

De forma destacada, la contestación del multilateralismo se enmarca en la creciente rivalidad geopolítica, comercial y tecnológica entre Estados Unidos y China. El esfuerzo de Estados Unidos por consolidar alianzas y retomar cierto liderazgo en la gobernanza global forma parte de este pulso entre ambas potencias.

La expansión económica de China, junto con un mayor proteccionismo de Estados Unidos, han provocado una creciente tensión en sus relaciones comerciales. Esta situación se ha materializado en una escalada de medidas arancelarias y restricciones a la exportación y la inversión adoptadas por ambas potencias.

La disputa es particularmente intensa en el ámbito tecnológico, donde se está produciendo una carrera por la supremacía mundial, que incluye el control de exportaciones

de tecnologías críticas y de doble uso. China, que ha logrado un gran desarrollo en la tecnología 5G y la Inteligencia Artificial busca alcanzar una posición de preeminencia que le permita definir los estándares y protocolos técnicos e industriales, así como ostentar el liderazgo en inversiones extranjeras directas en los operadores de redes y servicios.

Esta competición podría dar lugar a una brecha digital y productiva que desemboque en el desarrollo paralelo, pero diferenciado, de dos bloques tecnológicos. De esta forma, podría producirse un escenario de desacoplamiento en el que las cadenas de suministro de sectores estratégicos serían repatriadas o sometidas a un mayor control.

Adicionalmente, China ha redoblado sus esfuerzos por aumentar su peso en las organizaciones internacionales, con el objetivo de alcanzar una posición que le permita influir en las reformas de la gobernanza global. En términos globales, su capacidad de influencia relativa a la de Estados Unidos ha aumentado significativamente en las últimas tres décadas y ha logrado suplantar la influencia de países occidentales en muchas regiones, particularmente de África y del Sudeste Asiático.

En este panorama de tensión, Rusia se ha esforzado en los últimos años por lograr una posición de mayor liderazgo en la escena internacional, apostando por la multipolaridad, el reconocimiento a su «singularidad» y el reparto de áreas de influencia. La política expansionista de Rusia se ha visto reflejada en sus intervenciones en Siria y Libia y en su acercamiento a potencias con aspiraciones regionales como Turquía, India o Irán.

Al mismo tiempo, el orden nuclear heredado de la guerra fría se ha visto erosionado con el desmantelamiento de varios de los acuerdos de control de armas que limitaban la carrera armamentística entre Estados Unidos y Rusia, como el Tratado sobre Fuerzas Nucleares de Alcance Intermedio (INF). Sin embargo, Estados Unidos ha firmado un acuerdo con Rusia que renueva el Tratado de Reducción de Armas Estratégicas, conocido como New START. Además, ha indicado su interés en un retorno al Plan de Acción Integral Conjunto (PAIC) sobre el programa nuclear iraní, del que se retiró en 2018.

Potencias regionales, como Irán o Turquía, también han reforzado su influencia geopolítica en un contexto de fragmentación global y conflictos regionales, sobre todo en Oriente Medio y el Mediterráneo. Es posible que los conflictos en Palestina, Israel, Libia, Irak, Siria o Yemen continúen siendo escenarios de enfrentamiento entre diferentes actores estatales y no estatales, tanto nacionales como extranjeros.

La retirada de Estados Unidos y de la OTAN de Afganistán tras 20 años de presencia continua abre otro frente de competición geoestratégica, además de significar un posible uso del territorio afgano como refugio y base de acciones terroristas por parte de grupos yihadistas.

Por otro lado, la inestabilidad generada en el Mediterráneo oriental por las prospecciones gasísticas en el mar territorial en disputa entre Turquía, Chipre y Grecia muestra una tendencia a la unilateralidad en los litigios marítimos, dificulta una postura común de la Unión Europea y aumenta la dificultad de consenso dentro de la OTAN.

África subsahariana se está convirtiendo en escenario de rivalidades entre distintas potencias extrarregionales. En el Sahel, la desestabilización causada por el terrorismo yihadista se solapa con conflictos intercomunitarios en Estados que carecen de fortaleza institucional para hacer frente con éxito a este desafío múltiple. Todas estas dinámicas, unidas a la pobreza y desigualdad, agudizan la inseguridad imperante en varios países de la región.

Por su parte, la Unión Europea continúa su apuesta por una sólida relación transatlántica, al tiempo que define su postura hacia China entre la competición y la cooperación, en un ambiente de creciente inestabilidad en su vecindario oriental.

En este contexto multipolar y competitivo, se incrementa la necesidad de reforzar la autonomía estratégica de la Unión Europea, tanto en términos de política comercial e industrial comunitaria como en el desarrollo pleno de su Política Exterior y de Seguridad Común. Para ello, tendrá que lograr un equilibrio acorde con los compromisos de Derecho Internacional sobre la protección y garantía de los derechos humanos y con su papel como defensora de la democracia, el libre comercio y el multilateralismo.

Escenario socio-económico

La pandemia de la COVID-19 desencadenó la peor crisis económica mundial desde la Segunda Guerra Mundial, con una caída sin precedentes del Producto Interior Bruto (PIB) y de la actividad laboral mundial. La magnitud de sus efectos ha sido muy desigual, en función del tejido productivo de cada país, de los recursos económicos y de sus niveles de endeudamiento.

La repercusión de la crisis sobre la economía global en términos de PIB ha sido mayor que la de 2008, aunque ha estado seguida de un pronunciado repunte alcista. En un contexto de reducido crecimiento de la productividad en Europa y Estados Unidos, el impacto sobre las economías ha sido notable y podría acelerar el cambio en el equilibrio de poder de oeste a este. China es la única economía del G20 que no sufrió una recesión en 2020.

Si bien se espera que las consecuencias económicas negativas sean transitorias y que estén seguidas de tasas de crecimiento relativamente elevadas, se prevé un periodo de endeudamiento alto, fruto de las medidas extraordinarias de apoyo a ciudadanos y empresas adoptadas por la Unión Europea para hacer frente a la crisis.

En este sentido, la Unión Europea ha puesto en marcha un ambicioso Fondo de Recuperación y Resiliencia como respuesta común al proceso de transformación económica. El mecanismo Next Generation EU cuenta con 750.000 millones de euros financiados mediante la emisión de deuda comunitaria, que se suman a los 1.074 billones de euros del Marco Financiero Plurianual 2021-2027 para promover la recuperación económica y social y para favorecer un entorno de estabilidad y seguridad.

La crisis también ha puesto de relieve la dependencia del abastecimiento exterior de suministros estratégicos hay que añadir la puesta en marcha, por parte de los Estados, de políticas industriales estratégicas para hacer frente a la elevada competición global en determinados sectores tecnológicos e industriales.

La pugna económica y comercial entre las grandes potencias incluye el uso de los aranceles como instrumento de geopolítica, con su consiguiente impacto sobre las economías de la Unión Europea.

La súbita ralentización de la economía, el aumento de la desigualdad, la brecha digital, la destrucción de tejido productivo y el cierre de pequeñas y medianas empresas han derivado en un incremento de la pobreza y del nivel de frustración, marginalidad y exclusión social. Las clases medias, tras una década de crecimiento, se están contrayendo, mientras se expande la franja de población con ingresos bajos o muy altos. Este vaciamiento de las clases medias podría tener importantes consecuencias como el impacto negativo en el consumo global y el potencial incremento de populismos y autoritarismos identitarios, que podrían verse agravadas por los efectos de la automatización de los empleos. En este sentido, es preciso abordar un nuevo contrato social, para paliar la desigualdad y mitigar el proceso de precarización de las clases medias.

En algunos países, la crisis económica ha estado acompañada de una crisis social y política, alentada por campañas de desinformación y desestabilización que pretenden erosionar las instituciones, influir en los procesos democráticos y alentar la polarización.

Ante este escenario, la transformación digital y la transición ecológica cobran especial trascendencia como palancas de cambio de la estructura productiva de las economías mundiales y, en consecuencia, del mapa geopolítico. La digitalización y la economía verde habrán de avanzar de manera acompasada, de manera que la tecnología contribuya a alcanzar objetivos ecológicos y las tecnologías digitales minimicen su consumo energético y sus emisiones.

Transformación digital

El incremento de infraestructuras y servicios digitales, potenciado por tecnologías disruptivas y emergentes como la computación en la nube, la computación cuántica, la Inteligencia Artificial la virtualización de redes o el Internet de las Cosas, implica una transformación digital imparable que ofrece innumerables oportunidades de futuro, pero también presenta serios desafíos para la Seguridad Nacional.

En este contexto, la pandemia de la COVID-19 supuso una aceleración del proceso de digitalización, que ha situado a la interacción digital en el centro de las actividades públicas, privadas y profesionales y ha consolidado la hiperconectividad como rasgo definitorio redes y los sistemas de información y comunicaciones.

La digitalización de todo tipo de actividades ha ampliado la superficie de exposición a posibles ciberataques de organizaciones, tanto públicas como privadas, y ha dificultado la adecuada protección de la información. La magnitud y frecuencia de los ciberincidentes y del uso ilícito del ciberespacio han aumentado en los últimos años y han convertido la ciberseguridad en una prioridad de organizaciones y gobiernos.

Esta transformación digital no es un fenómeno solo tecnológico, sino que tiene impacto en las relaciones sociales y la configuración geopolítica. Los cambios tecnológicos generan cambios de poder, tanto dentro de los Estados como entre ellos. Con la consolidación del ciberespacio como dominio estratégico, se acentuará la brecha tecnológica tanto entre individuos y sociedades como entre países.

La estabilidad económica y las políticas monetarias también se ven afectadas por la irrupción de tecnologías potencialmente disruptivas. En particular, la configuración actual del sistema financiero global puede verse desafiada por la implantación de divisas digitales.

En este ámbito, los riesgos se ven amplificados por la prevalencia de criterios comerciales frente a los de seguridad en el diseño de productos de hardware y software, así como de sistemas y servicios, tales como el 5G. Este hecho dificultad los procesos de certificación y puede comprometer la cadena de suministro, especialmente en la provisión de servicios esenciales y/o críticos.

Otros riesgos, pero también múltiples oportunidades, derivan de los avances tecnológicos en campos como la biotecnología, que han facilitado el rápido desarrollo de vacunas eficaces contra la COVID-19, pero plantean interrogantes éticos ante actividades como determinados empleos de la ingeniería genética.

Por otro lado, la vulnerabilidad ante posibles injerencias de terceros es extensible al dominio de infraestructuras digitales, como los centros de procesamiento de datos o los cables submarinos, y a los activos que sustentan la propiedad intelectual e industrial del sector empresarial. También habrá que considerar el mapa mundial de conectividad y la aparición de nuevos operadores satelitales, especialmente aquellos vinculados a las grandes empresas tecnológicas.

Con el dato convertido ya en un recurso estratégico de primer orden, se ha intensificado el debate sobre la ética y la defensa de derechos digitales, condicionado especialmente por la concentración de la información en las grandes compañías tecnológicas y por su uso abusivo por parte de algunos actores políticos. En este debate, el derecho a la privacidad de los usuarios de servicios digitales ocupa un lugar central y ha dado lugar a pronunciamientos judiciales que podrían condicionar el desarrollo tecnológico.

El acceso seguro a los servicios públicos y privados, en particular a los servicios esenciales en línea, supone que la ciudadanía pueda proteger su identidad y controlar los datos que comparte y cómo se utilizan, de manera que se garantice la privacidad y la protección de datos personales. Disponer de una identidad digital segura es una pieza clave para la ciberseguridad.

La gobernanza democrática sobre el futuro digital es de máxima importancia para resolver las inquietudes relativas a los derechos y libertades y a la competición geopolítica.

Transición ecológica

La crisis climática ha dado paso a una mayor concienciación política y social de la necesidad de luchar contra sus consecuencias a través de procesos de transición ecológica.

El cambio climático tiene un impacto negativo en la vida y el bienestar humano. Entre sus efectos se encuentran el incremento en el número de fenómenos meteorológicos extremos, la degradación de ecosistemas terrestres y marinos, la desertificación, el aumento de la incidencia y frecuencia de olas de calor, las sequías, la reducción de las disponibilidades de agua, las intrusiones de polvo sahariano, los incendios forestales e inundaciones y la pérdida de la biodiversidad. Estos efectos perniciosos podrían llevar a una mayor competencia por los recursos y al incremento de desplazamientos migratorios desde zonas más expuestas a las consecuencias dañinas del cambio climático.

Por otro lado, la degradación de la biodiversidad produce la pérdida de sus servicios ecosistémicos, esenciales para el bienestar e incluso la supervivencia del ser humano, y propicia la expansión de especies exóticas invasoras, responsables de impactos relevantes en la economía y potenciales vectores de nuevas enfermedades.

En este contexto, la adaptación al cambio climático es básica para conseguir una resiliencia ambiental y ecológica que preserve la vida y el bienestar de la sociedad y el medio.

En diciembre de 2019, la Unión Europea presentó el Pacto Verde Europeo, una hoja de ruta para hacer que su economía sea sostenible y neutral climáticamente en 2050. Para ello, se ha establecido el objetivo vinculante de conseguir, en 2030, una reducción interna neta de emisiones del 55% respecto a los niveles de 1990. En este marco, es igualmente importante el impulso hacia una economía circular con un modelo de producción y consumo basado en reutilizar, renovar y reciclar materiales y productos. Este modelo ayudará a reducir la presión sobre el medio ambiente, a mejorar la seguridad de las cadenas de suministro mediante un empleo más efectivo de los recursos existentes y a estimular el desarrollo empresarial en el campo de la I+D+i.

Un aspecto clave para lograr la neutralidad climática es el cambio del paradigma energético, que transita de la dependencia de los combustibles fósiles a la de las tecnologías renovables. Esto propiciará una nueva geopolítica de transición energética y un cambio en el equilibrio entre importadores y exportadores.

El desarrollo de energías renovables tiene además un carácter estratégico, ya que permitirá el uso de fuentes autóctonas y una mayor diversificación, lo que incrementa la seguridad y mejora la balanza exterior. Sin embargo, también conlleva importantes desafíos tecnológicos relacionados con un sistema de generación eléctrica basado en fuentes de energía variable, el desarrollo de nuevos sistemas de almacenamiento e infraestructuras inteligentes, así como retos relacionados con la reducción del impacto sobre el medio natural y humano.

La evolución hacia una economía descarbonizada incrementará la competencia por las materias primas, como las tierras raras, los materiales y procesos industriales relacionados con la digitalización y las tecnologías renovables, así como una mayor dependencia de las regiones geográficas abastecedoras de estas tecnologías.

CAPÍTULO 2

Una España segura y resiliente

El segundo capítulo de la Estrategia de Seguridad Nacional ofrece un recorrido de las distintas regiones geográficas del mundo desde la perspectiva española de la seguridad.

España es un Estado social y democrático de Derecho, dotado de un marco constitucional de derechos y libertades que tiene al ciudadano como eje central, con unas instituciones sólidas y plenamente democráticas. Una de sus principales fortalezas reside en su sociedad plural, abierta y solidaria.

La visión de futuro de una España segura y resiliente incluye la transformación tecnológica y la transición ecológica como vectores que faciliten un crecimiento sostenible y justo, la competitividad del tejido industrial y empresarial y la creación de empleo de calidad.

La Seguridad Nacional debe contribuir a la cohesión territorial y es necesario asegurar que todas sus estructuras sean más resilientes frente a los riesgos y las amenazas.

Desde una perspectiva geográfica, la configuración de España es singular, con una dimensión territorial peninsular, archipiélagos, islas, peñones y las Ciudades Autónomas de Ceuta y Melilla en el norte de África, además de una significativa extensión marítima.

Su posición le confiere la condición de país europeo, mediterráneo y atlántico que se proyecta al mundo como un contribuyente comprometido con la paz y la seguridad internacional. España defiende el refuerzo del multilateralismo, la profundización en la construcción europea, las alianzas bilaterales estratégicas y el compromiso solidario como principios establecidos en la Estrategia de Acción Exterior. La cooperación con los vecinos fronterizos, Francia, Andorra, Portugal y Marruecos es especialmente relevante.

La Estrategia de Seguridad Nacional está alineada con los objetivos de las organizaciones a las que España pertenece, especialmente las Naciones Unidas, la Unión

Europea y la OTAN, con las que pretende proteger y garantizar los intereses compartidos con sus socios y aliados.

Europa

España es un Estado miembro con peso dentro de la Unión Europea, firme defensor del avance en la construcción europea y proactivo en el desarrollo de políticas comunes en áreas de especial relevancia como la energía, la inmigración y la seguridad.

Para España, una Unión más resiliente es una Europa más fuerte en el mundo. La Unión Europea debe seguir avanzando en el desarrollo de su Política Exterior y de Seguridad Común, en especial de su Política Común de Seguridad y Defensa, frente a desafíos derivados del empleo de estrategias híbridas y de posturas adversas de actores como Rusia y China o de fenómenos como el terrorismo, así como en la coordinación y cooperación con la OTAN y las Naciones Unidas.

La protección de los espacios y rutas marítimas es clave para la seguridad europea. El margen atlántico es un área de interés estratégico que conecta Europa con todo el continente americano y con África occidental. El progresivo deshielo del Ártico abre nuevas rutas marítimas con implicaciones estratégicas. Además, España comparte agenda en áreas como el golfo de Guinea, con otros países europeos atlánticos, como es el caso de Francia y Portugal, principalmente en relación con la seguridad marítima y energética.

Al sur de Europa, el mar Mediterráneo es un nexo común y un puente estratégico con África y Oriente Medio, pero también un escenario de tensión y fricción donde distintos países y actores pretenden imponer su criterio y sus intereses, en ocasiones de espaldas al Derecho Internacional y violando la soberanía de los Estados ribereños.

En este sentido, España trabajará para promover el diálogo en torno al Mediterráneo oriental, de acuerdo con la perspectiva de la Unión Europea y en el entendimiento de que Turquía es un actor regional clave, un aliado en la OTAN y un socio estratégico con intereses compartidos.

En el flanco oriental, la posición cada vez más asertiva de Rusia ha tensionado sus relaciones con la Unión Europea, que además ha constatado el desafío que suponen algunas de las acciones procedentes de ese país, tanto militares como híbridas. España seguirá apostando por mantener el diálogo con Rusia, a pesar de las dificultades, sobre la premisa del respeto al Derecho Internacional, la defensa de la soberanía y la integridad territorial de los Estados y el respeto a los derechos humanos en su acción exterior.

La salida de Reino Unido de la Unión Europea ha modificado el escenario europeo y presenta retos relacionados con la pérdida de un gran activo en el ámbito de la seguridad. Para España, esta salida no impedirá fortalecer los vínculos entre dos países amigos y aliados. No obstante, y desde la base de una cooperación positiva, España no renuncia a la oportunidad que se abre con este nuevo escenario para solventar el anacronismo que representa la situación de Gibraltar.

Magreb y Oriente Próximo

La prioridad de España en el Magreb es promover un espacio de seguridad, estabilidad política y desarrollo y contribuir a enfrentar amenazas, como el terrorismo o el crimen organizado, desde un enfoque de colaboración con países que son socios y amigos preferentes de España.

La relación de España con Marruecos y Argelia es de buena amistad, desde la premisa de la cooperación leal y el respeto a las fronteras mutuas. La colaboración con estos países en aspectos relacionados con la seguridad, como los tráficos ilegales o el terrorismo, complementa unas sólidas relaciones basadas en el diálogo político, las relaciones comerciales y los vínculos energéticos.

El apoyo a la convulsa democracia en Túnez y la contribución a los esfuerzos liderados por las Naciones Unidas para solventar la crispada situación que atraviesa Libia son también imprescindibles para lograr la paz y la estabilidad en el Mediterráneo.

La región de Oriente Próximo es un foco de atención internacional por su persistente inestabilidad, pero también por la proliferación de conflictos internos, la extensión del terrorismo yihadista, las graves crisis humanitarias y la injerencia de determinados actores

globales y regionales al margen de marcos multilaterales. La guerra en Siria y Yemen y la tensión entre Irán y las monarquías del Golfo dibujan un panorama complejo. Por otro lado, el repliegue de Estados Unidos de determinados escenarios de Oriente Próximo dejará un vacío que será aprovechado por actores como Rusia y China. Enfrentar todos estos desafíos exige una firme y amplia cooperación internacional.

España es un país comprometido con la seguridad de la región, con militares desplegados tanto en el Líbano, en el marco de las Naciones Unidas, como en operaciones de la OTAN, la Unión Europea y la Coalición Global contra el Daesh.

España ha apoyado de manera activa, desde la conferencia de Paz de Madrid en 1991, una solución al conflicto palestino-israelí a través del Proceso de Paz en Oriente Próximo. Los acuerdos entre Israel y Emiratos Árabes Unidos, Bahréin y Marruecos en 2020 muestran la rapidez y profundidad de los cambios en la región, así como la necesidad de adaptar la posición española para que siga siendo útil en la búsqueda de una solución justa con ambas partes.

África Subsahariana

El nexo seguridad-desarrollo y un enfoque preventivo son los principios que guían las políticas para la contribución de España a la estabilidad en tres áreas geográficas de especial interés: el Sahel, el golfo de Guinea y el Cuerno de África, tal y como se recoge tanto en el III Plan África como en el programa Foco África 2023.

España mantendrá el apoyo a las iniciativas de seguridad internacionales y regionales, así como su compromiso con las misiones civiles y militares de la Unión Europea en África.

En el Sahel, la permanente crisis de gobernabilidad y la ausencia del Estado en grandes espacios de soberanía se suman a emergencias humanitarias por desastres naturales o por los efectos adversos del cambio climático. Todo ello en un entorno de fragilidades estructurales que, unidas a la presión sobre los limitados recursos para una población caracterizada por su elevado crecimiento demográfico, han exacerbado amenazas latentes como son el terrorismo yihadista, los numerosos conflictos intercomunitarios o los tráficos ilícitos. Además, los factores de inestabilidad del Sahel, y en particular la amenaza del extremismo violento, se extienden hacia los países costeros de África occidental y norte de África.

Los países del golfo de Guinea tienen una gran importancia estratégica para Europa y para la salvaguardia de los intereses españoles. En sus espacios marítimos proliferan actividades delictivas como los secuestros y el robo a mano armada en los buques pesqueros y petroleros, o la piratería y la pesca ilegal en aguas internacionales. En el golfo de Guinea, España contribuye activamente a una navegación segura en las rutas y espacios marítimos, con el objetivo de fortalecer la seguridad marítima nacional y regional a fin de garantizar también el suministro energético, la protección de la pesca y las inversiones españolas en la región.

En el Cuerno de África, la aplicación de un enfoque integral que aborde las raíces de los conflictos que afectan a rutas y espacios marítimos de alta importancia internacional seguirá orientando la acción de España. Además, España sigue con preocupación los acontecimientos en el norte de Mozambique, que representan un foco de inestabilidad para la región en su conjunto.

América del Norte y el Vínculo Transatlántico

La alianza estratégica de España con Estados Unidos está basada en una relación de mutua confianza a con dimensiones políticas, económicas, culturales y militares. El Convenio de Cooperación para la Defensa, suscrito entre ambos países, constituye un valor añadido, sin olvidar tampoco la buena colaboración, junto a otros socios y aliados, en el seno de la Coalición Global contra el Daesh.

El escenario actual abre una ventana de oportunidad para la consolidación del vínculo transatlántico y el refuerzo y reforma del multilateralismo y sus instituciones. También se ha de tener en consideración el giro estratégico de Estados Unidos hacia el Indo-Pacífico y su presencia más reducida en Oriente Medio. España, miembro de la Unión Europea y de la

OTAN, apoyará la cooperación entre las dos organizaciones como eje central de la seguridad colectiva frente a los grandes desafíos globales.

América Latina y el Caribe

América Latina ha experimentado un rápido desarrollo en la primera década del siglo XXI. Sin embargo, enfrenta aún importantes desafíos, que se han agudizado por efecto de la pandemia de la COVID-19: inseguridad ciudadana, crisis medioambientales y desastres naturales, altos índices de corrupción, tráficos ilícitos y crimen organizado.

España fomentará la unión y la estabilidad en América Latina a través de la acción bilateral, los foros regionales y las Cumbres Iberoamericanas. Además, redoblará sus esfuerzos para servir de puente de entendimiento y colaboración con la Unión Europea y fomentar la colaboración en la gestión de crisis que afectan a todos.

España seguirá colaborando con la erradicación de la producción y el tráfico de drogas desde América Latina, por la amenaza que supone para la región y por ser España uno de los puntos de entrada a Europa de estos tráficos ilícitos.

España también se esforzará en mantener su privilegiada relación con América Latina sobre la base de una cooperación reforzada y una relación más estrecha en el ámbito de la Defensa, especialmente a través de la cooperación en operaciones de apoyo a la paz, en el nivel bilateral y regional.

Asia-Pacífico

El progresivo desplazamiento del centro de gravedad económico y estratégico mundial hacia el área de Asia-Pacífico hace que sea una zona de interés para España.

La Unión Europea ha señalado su compromiso con la estabilidad y prosperidad en la región del Indo-pacífico, un área geográfica clave para la seguridad internacional que está experimentando una creciente competición geopolítica.

Los litigios marítimos en el mar del sur de China, las tensiones en torno a Taiwán, el conflicto sobre Cachemira o las disputas fronterizas entre India y China introducen elementos de inestabilidad regional, que se suman a amenazas como el desarrollo de armas y vectores nucleares en la República Popular Democrática de Corea o la expansión del terrorismo transnacional de carácter yihadista.

Países como India y China ocupan cada vez mayor espacio en los asuntos internacionales. Por otro lado, iniciativas regionales como el Acuerdo de Asociación Económica Integral Regional amplifican la influencia de la región en la economía mundial.

El ascenso de China como potencia global se proyecta a través de su nueva ruta de la seda, su dominio tecnológico y una creciente presencia inversora en América Latina y África, así como en países europeos. En su relación con Pekín, la Unión Europea combina elementos de rivalidad sistémica, áreas de competición y retos globales comunes, como el cambio climático o la no proliferación de armas nucleares, que requieren cooperación.

La situación en Afganistán tras la retirada de Estados Unidos podría tener un impacto geopolítico significativo con la posible reconfiguración de las relaciones tanto a nivel global como regional. El potencial deterioro de la situación humanitaria y de derechos humanos presenta un desafío adicional. Además, para la seguridad de Europa será especialmente importante evitar que el país vuelva a convertirse en un santuario para terroristas y un foco de crimen organizado.

España apoya las iniciativas de refuerzo de la cooperación en la región en áreas como la conectividad y la seguridad marítima, así como la acción concertada frente a desafíos de dimensión global, como el cambio climático y la salud, y el impulso de las relaciones comerciales. Además, profundizará las relaciones con aquellos países de la región con los que comparte valores e intereses.

CAPÍTULO 3

Riesgos y amenazas

El tercer capítulo de la Estrategia de Seguridad Nacional describe un mapa de los riesgos y amenazas a la Seguridad Nacional con un enfoque que pone de relieve su

dinamismo e interdependencia, en un entorno de seguridad donde las estrategias híbridas ganan protagonismo.

El panorama actual de seguridad es más incierto que en años anteriores. La crisis de la COVID-19 ha intensificado las tendencias globales de fondo y ha acelerado el ritmo de transformación.

La superficie de confrontación geopolítica encuentra áreas de intersección con la tecnología y la economía, dibujando así un mapa de riesgos más complejos y muy interrelacionados. Adicionalmente, amenazas derivadas del uso de tecnologías de nueva generación, como la Inteligencia Artificial o el acceso al espacio ultraterrestre, añaden complejidad y dificultan la protección de los derechos individuales ante un eventual uso malicioso.

En esta Estrategia, los factores que afectan a la Seguridad Nacional se plantean como elementos de un continuo que refleja una gradación progresiva en función de su grado de probabilidad e impacto. Así, los riesgos y las amenazas no son estáticos, sino que se conciben de una manera dinámica.

Además, se presenta un mapa de riesgos con dos características diferenciales con respecto a modelos anteriores. Por un lado, se subraya el papel primordial de la tecnología en la mayoría de las amenazas y la prominencia de las estrategias híbridas y, por otro, se acentúan las interconexiones entre los distintos riesgos y amenazas. De esta forma, la interrelación entre ellos puede producir efectos en cascada, como ha ocurrido con la crisis generada por la pandemia.

Con este planteamiento, es importante contar con las capacidades necesarias para responder a una amalgama de riesgos y amenazas, en lugar de prepararse solamente para una posible repetición de una crisis similar a la ya experimentada.

Tensión estratégica y regional

En el contexto de seguridad actual, caracterizado por un retroceso del multilateralismo, un aumento de la asertividad de ciertos actores y un incremento de la competición estratégica entre Estados, el riesgo de que se produzcan tensiones con impacto directo sobre los intereses nacionales e incluso sobre la propia soberanía, constituye una seria amenaza para la Seguridad Nacional, cuya máxima expresión podría llegar a adoptar la forma de conflicto armado.

Esta situación se ve agravada por la fragilidad y vacíos institucionales en algunas regiones próximas, cuyos conflictos internos pueden, igualmente, afectar a los intereses de España. Estos escenarios de inestabilidad, si no son contenidos a tiempo, pueden tensionar aún más las relaciones internacionales, elevando el riesgo de conflictos entre Estados a nivel regional.

En este clima de creciente tensión internacional, donde determinados actores se rearman para fortalecer sus aspiraciones estratégicas, España requiere una capacidad de disuasión creíble y efectiva y una capacidad de defensa autónoma, frente a diferentes formas de agresión: desde las estrategias híbridas hasta el conflicto convencional. España debe, además, seguir siendo un socio comprometido y fiable de la Unión Europea, la OTAN, las Naciones Unidas y otros marcos multinacionales de seguridad y defensa.

En este contexto y debido a la naturaleza cambiante de los conflictos, los tradicionales dominios terrestre, naval y aéreo, se ven ahora complementados por la aparición de nuevos espacios de competición, como el ciberespacio y el espacio ultraterrestre, que obligan a incorporar nuevas formas de actuación, así como tecnologías de última generación para mantener una capacidad de enfrentamiento actualizada y moderna.

Terrorismo y radicalización violenta

La polarización y la crisis económica han contribuido a un incremento en la actividad de los extremismos violentos.

Los medios utilizados por los grupos terroristas son cada vez más variados y los ataques físicos están acompañados de campañas propagandísticas que alimentan ideologías radicales violentas.

En esta amenaza cobra especial relevancia el terrorismo yihadista, con su presencia tanto en distintos países europeos, como en el Sahel, Magreb y Oriente Medio, desde donde se proyecta la amenaza terrorista sobre España. Existe además el riesgo de ataque sobre individuos e intereses nacionales en estas regiones.

Dentro de las fronteras de España, la principal amenaza proviene de individuos que han nacido o crecido en países occidentales que, tras ser radicalizados, atacan en su propia área de residencia. Igualmente relevante es la amenaza derivada de los procesos de radicalización en prisiones.

Además, el posible retorno de personas desplazadas a zonas de conflicto para apoyar a los grupos terroristas constituye un riesgo significativo. Por ello, es necesario fortalecer la cooperación y colaboración en materia antiterrorista y judicial, no solo entre los Estados miembros de la Unión Europea, sino también con terceros países, bajo un enfoque multidisciplinar.

Epidemias y pandemias

La crisis desencadenada por la COVID-19, además de cobrarse la vida de millones de personas en el mundo, ha tenido importantes consecuencias sociales y económicas, con un impacto desigual que ha agudizado las brechas existentes entre países, sociedades y ciudadanos.

Las dificultades experimentadas por los organismos internacionales para la toma de decisiones y las tensiones surgidas en relación con la producción y distribución de material sanitario, fármacos o vacunas dirigidos a combatir la enfermedad han contribuido a intensificar fricciones geopolíticas existentes y, en determinados casos, a dificultar la cooperación internacional.

Un aspecto crucial que se ha puesto de manifiesto es la fragilidad de las cadenas de suministro global de determinados recursos estratégicos y la necesidad de disminuir el grado de dependencia del exterior de recursos esenciales para garantizar su accesibilidad en todo momento.

Amenazas a las infraestructuras críticas

Las Infraestructuras Críticas posibilitan el normal desarrollo de la actividad socio-económica y son objetivo de amenazas, tanto físicas como digitales, que podrían llevar a una interrupción o negación de servicios.

La progresiva digitalización y la adopción de nuevas tecnologías por parte de los operadores críticos y operadores de servicios esenciales podría aumentar el riesgo de sufrir brechas de seguridad, que permitirían acceder al control de los sistemas que operan las Infraestructuras Críticas y poner en peligro la continuidad de los servicios que proveen.

Otro riesgo a considerar es la potencial pérdida de control sobre la capacidad de decisión estratégica a raíz de inversiones por actores, estatales o no estatales, con intereses no necesariamente alineados con la Seguridad Nacional.

Emergencias y catástrofes

La seguridad de las personas y los bienes se ve afectada por distintos tipos de emergencias y catástrofes originadas por causas naturales o derivadas de la acción humana accidental o intencionada.

Factores potenciadores del riesgo de emergencias y catástrofes son tanto la despoblación rural como la sobrepoblación de algunas ciudades, la degradación del ecosistema agravada por los efectos del cambio climático o el incremento en la magnitud y frecuencia de algunos fenómenos meteorológicos adversos.

En este contexto, se identifican como principales riesgos las inundaciones, los incendios forestales, los terremotos y maremotos, los riesgos volcánicos, los fenómenos meteorológicos adversos, los accidentes en instalaciones o durante procesos en los que se utilicen o almacenen sustancias peligrosas, el transporte de mercancías peligrosas por carretera y ferrocarril, los accidentes catastróficos en el marco del transporte de viajeros y los riesgos nucleares, radiológicos y biológicos.

Espionaje e injerencias desde el exterior

El incremento de la competitividad y de la tensión en el escenario internacional ha supuesto un aumento de las injerencias desde el exterior que España debe confrontar. Entre las herramientas más eficaces de algunos países que aspiran a expandir su influencia internacional destacan las actividades de espionaje.

La pertenencia de España a organizaciones como la Unión Europea y la OTAN, hacen del país un objetivo atractivo. Sin embargo, los objetivos de los Servicios de Inteligencia hostiles no se limitan a las instituciones y a la información del Gobierno de España, también afectan a otros sectores, como por ejemplo a la industria de defensa, las Infraestructuras Críticas o la investigación científica y tecnológica, así como a otros ámbitos del sector privado. Estas actividades no solo son críticas para la Seguridad Nacional, sino que pueden atentar contra la competitividad económica y la propiedad intelectual, especialmente en lo que respecta a los sectores estratégicos y al campo de la ciencia y la investigación.

Asimismo, son destacables los esfuerzos de algunos actores extranjeros por influir sobre sus nacionales asentados en España, afectando a los derechos y libertades de los ciudadanos y, potencialmente, a la estabilidad social.

En otras ocasiones, las actuaciones de los Servicios de Inteligencia extranjeros no tienen como objetivo intereses españoles o aliados, sino que utilizan el territorio español como base de sus operaciones en otros países, pudiendo atentar contra la soberanía nacional.

Tanto las actividades de inteligencia clásicas como el ciberespionaje son una importante amenaza en sí mismos. Pero, además, hay que considerar que las actividades de los Servicios de Inteligencia hostiles pueden formar parte de las llamadas estrategias híbridas. Dentro de estas estrategias, las actividades de espionaje pueden llegar a ser un elemento destacable y potencian la amenaza que suponen para la Seguridad Nacional.

Campañas de desinformación

Las campañas de desinformación tienen clara repercusión en la Seguridad Nacional y deben diferenciarse de otros factores como la información falsa –*fake news*– o información errónea –*misinformation*–. De hecho, las campañas de desinformación no contienen necesariamente noticias falsas, sino que pretenden distorsionar la realidad mediante contenido manipulado.

En este sentido, el ámbito cognitivo es un espacio más en el que ejercer influencia, que se suma a los tradicionales ámbitos físicos: terrestre, marítimo y aéreo. Los elementos que sí son inherentes a una campaña de desinformación son la voluntad de generar confusión y socavar la cohesión social; el uso coordinado de distintos medios para la creación y difusión de contenidos dirigidos a audiencias amplias; y la intención maliciosa con fines de desprestigio o influencia sobre el objetivo del ataque. Así, las campañas de desinformación suponen una grave amenaza para los procesos electorales.

Por su potencial peligrosidad, cabe señalar las estrategias de desinformación de actores extranjeros, tanto estatales como no estales, que desarrollan aparatos de propaganda con la intención de polarizar a la sociedad y minar su confianza en las instituciones.

Vulnerabilidad del ciberespacio

Se distinguen dos tipologías generales de amenazas en el ciberespacio. Por un lado, los ciberataques, entendidos como acciones disruptivas que actúan contra sistemas y elementos tecnológicos. Ejemplos de ello son los ataques de *ransomware* (secuestro de datos) o la denegación de servicios, entre otros. Y, por otro lado, el uso del ciberespacio para realizar actividades ilícitas, como el cibercrimen, el ciberespionaje, la financiación del terrorismo o el fomento de la radicalización.

La creciente exposición digital amplía la superficie de exposición a ciberataques de ciudadanos, empresas y administraciones. Entre las dinámicas que marcan un mayor revolución industrial, el despliegue de las redes 5G multiplicará la capilaridad de las redes y con ello aumentará de manera significativa su uso, no solo por usuarios sino en el segmento Internet de las Cosas y las comunicaciones máquina-a-máquina. Consecuentemente, se generará un aumento de la vulnerabilidad ante ciberataques en aparatos conectados a la red y servicios como el vehículo autónomo o las redes inteligentes.

Asimismo, en la denominada sociedad virtual, el dato constituye un nuevo ámbito de poder que afecta tanto a la relación entre Estados como entre el sector público y el privado, al ser las compañías tecnológicas las que poseen un mayor acceso a los datos. La seguridad de la información afecta al ciudadano de forma directa. La regulación, protección y garantía del uso adecuado de los datos y las redes por las que transitan es un aspecto clave de la Seguridad Nacional, con impacto directo sobre la privacidad personal.

Tecnologías como la Inteligencia Artificial y el *big data* subyacen cada vez más en ámbitos como el sanitario, el de transportes, el energético, el empresarial, el financiero, el educativo y el militar. La capacidad de procesamiento de grandes cantidades de datos se presenta como una característica avanzada para la consecución de los objetivos deseados. Su potencial de transformación y aplicación en procesos de análisis de riesgos y de alerta temprana es cada vez mayor. Pero el desarrollo de estas tecnologías también genera interrogantes relacionados con la seguridad. La aplicación de algoritmos para la toma automática de decisiones requiere un marco de protección de la privacidad y la no-discriminación. El empleo de sistemas autónomos también tiene implicaciones éticas que requieren mecanismos de control y parámetros que garanticen el respeto a los derechos humanos.

En el medio-largo plazo, el salto tecnológico que supone la computación cuántica permitirá usos difíciles de prever hoy en día en materia de comunicaciones seguras, cifrado y descifrado y sistemas de vigilancia avanzados, entre otros.

Vulnerabilidad del espacio marítimo

El espacio marítimo es considerado uno de los espacios comunes globales, espacios de conectividad de flujos, información, personas, servicios y bienes, cuya interrupción u obstaculización puede tener un impacto económico severo.

Para España, país de condición marítima, es esencial mantener la seguridad en los espacios marítimos, así como asegurar el funcionamiento de las Infraestructuras Críticas situadas en el litoral y en el mar, como los puertos y tuberías submarinas y, especialmente, los cables submarinos, por los que circula la práctica totalidad del tráfico de datos. De su buen uso y estado depende, en gran medida, la economía, ya que los recursos energéticos y la mayor parte del comercio español transita por rutas marítimas.

La piratería y el robo a mano armada en la mar atentan contra la navegación segura por las principales rutas de tráfico marítimo y contra la flota pesquera de pabellón nacional, principalmente en la cuenca somalí, el golfo de Adén y el golfo de Guinea.

Además, los tráficos ilícitos, la explotación ilegal de los recursos marinos y los actos contra el patrimonio arqueológico subacuático son fenómenos perjudiciales para el sector marítimo.

Vulnerabilidad aeroespacial

El sector aeronáutico es de alta importancia estratégica. Cualquier disrupción que afecte a las aeronaves, los aeropuertos o las instalaciones en tierra, en especial un ataque terrorista, tendría un impacto de magnitud y trascendencia económica considerables.

La alta conectividad aérea entre países y continentes es, asimismo, una de las causas de la rápida propagación de enfermedades infecciosas a nivel internacional.

Una de las tendencias preocupantes es la proliferación del uso ilícito de vehículos aéreos no tripulados, que pueden paralizar el uso de aeropuertos o infraestructuras críticas, y son además potenciales armas para sabotajes o acciones terroristas.

El espacio ultraterrestre está considerado como la última frontera de confrontación geopolítica. Este espacio común global se ha convertido en un dominio de explotación comercial intensiva, con la proliferación de constelaciones de satélites y lanzadores comerciales. Sin embargo, algunos operadores, no radicados en la Unión Europea, están en el camino de alcanzar una posición de dominancia tal de los mercados que podría poner en riesgo tanto el acceso al espacio (lanzamientos) como a determinados servicios espaciales. En este sentido, las nuevas constelaciones de satélites pueden hacer insostenible el modelo de cooperación público-privada español en comunicaciones gubernamentales y observación de la Tierra.

Además, la falta de normativa legal facilita la actividad irregular en el espacio ultraterrestre y dificulta la protección de activos estratégicos, como las comunicaciones vía satélite, los sistemas de posicionamiento y tiempo o los satélites de observación terrestre. Por otro lado, la seguridad de los sistemas espaciales se verá seriamente afectada por el incremento de los desechos espaciales y la carencia de un sistema de gestión del tráfico espacial global.

Inestabilidad económica y financiera

La pandemia de la COVID-19 ha generado el mayor desplome del Producto Interior Bruto desde la Segunda Guerra Mundial, lo que ha causado una nueva crisis económica con consecuencias aún inciertas en clave social. Aunque el impacto económico sea fundamentalmente transitorio y esté seguido de tasas de crecimiento relativamente elevadas, ha causado un aumento de la situación de inestabilidad y desigualdad económica.

Entre los factores que pueden contribuir a la inestabilidad económica y financiera se incluyen los desequilibrios en las vías de financiación de la Hacienda Pública; la inestabilidad financiera internacional; el fraude, la evasión y la planificación fiscal; la corrupción; el blanqueo de capitales y el uso indebido de los fondos procedentes de subvenciones y contratos públicos. Estos factores socavan la seguridad económica y provocan desafección social de las instituciones gubernamentales.

Crimen organizado y delincuencia grave

El crimen organizado es una amenaza a la seguridad que se caracteriza por su finalidad esencialmente económica, su efecto horadador sobre la instituciones políticas y sociales, su carácter transnacional y su opacidad.

Los grupos delictivos y las organizaciones criminales camuflan sus operaciones ilegales con negocios lícitos y se apoyan cada vez más en tecnologías digitales, como las cripto-monedas y la Internet oscura.

Además de su dimensión económica, el crimen organizado tiene un relevante potencial desestabilizador. Sus estructuras se adaptan al entorno geoestratégico y repercuten en la gobernanza, la paz social y el normal funcionamiento de las instituciones.

En cuanto a la delincuencia grave, actividades como la explotación de menores o la trata con fines de explotación sexual se dirigen hacia los colectivos vulnerables y violan gravemente los derechos humanos. El contrabando, el cibercrimen, el tráfico de drogas, de armas y de especies silvestres y la corrupción son amenazas tangibles para la Seguridad Nacional.

La convergencia entre grupos terroristas y redes de crimen organizado va en aumento. Los modelos de organización cada vez más descentralizada de estos actores delictivos favorecen su cooperación y facilitan la financiación terrorista.

Flujos migratorios irregulares

El fenómeno de la migración contemporánea –global, complejo y multidimensional– tiende a difuminar las distinciones tradicionales entre países de origen, destino y tránsito. Los factores económicos, sociales y medioambientales, así como la inestabilidad política, la pobreza y los conflictos, seguirán influyendo en las tendencias migratorias mundiales. Asimismo, la multiplicación de las opciones de comunicación y desplazamiento favorecen una nueva era de movilidad humana. Junto a oportunidades, los movimientos migratorios seguirán generando retos –incluidos los de carácter securitario en sentido amplio– que hay que gestionar.

El desarrollo tanto en los países de origen como en los receptores de migrantes, se ve quebrado por las actividades ilícitas de organizaciones criminales dedicadas al tráfico y la trata de personas, que proliferan en torno a los movimientos migratorios y cuyas actividades conllevan graves vulneraciones de derechos humanos.

España, por su posición geoestratégica, está especialmente expuesta al desafío que supone el esperado aumento de los flujos migratorios hacia Europa en los próximos años. En su condición de frontera exterior de la Unión Europea, España afronta la gestión de los

flujos migratorios irregulares como un importante reto que requiere una política migratoria común, basada en el justo equilibrio entre solidaridad y responsabilidad compartida entre Estados. Los riesgos derivados de la inmigración irregular afectan directamente a la continuidad del espacio Schengen.

Vulnerabilidad energética

El proceso de transformación del sector energético lleva aparejado nuevos riesgos asociados a un modelo de generación verde. La disponibilidad de nuevas materias primas, las nuevas tecnologías de almacenamiento o la generación distribuida basada en energías renovables, el autoconsumo y la eficiencia son todos elementos a tener en cuenta en la ecuación energética actual.

La incorporación de medidas orientadas a garantizar la cohesión económica y territorial para paliar los efectos socioeconómicos de los cambios en las fuentes de energía primaria, como la transición justa, forman parte de la nueva visión de la seguridad energética en esta estrategia.

Si bien la dependencia de hidrocarburos provenientes del exterior seguirá siendo un factor de vulnerabilidad en los próximos años, la transición hacia un nuevo modelo energético económicamente sostenible y respetuoso con el medioambiente es el principal desafío de un sector clave para la economía y la seguridad, donde el cambio climático es considerado como un riesgo sistémico a nivel global.

Proliferación de armas de destrucción masiva

La modernización y el aumento del arsenal nuclear de China, India y Pakistán, junto con los avances del programa nuclear de la República Popular Democrática de Corea y el programa de enriquecimiento de uranio en Irán, contribuyen a diseñar un orden nuclear cada vez más multipolar. Este escenario podría desencadenar una nueva carrera armamentística definida por la posible reanudación de pruebas nucleares y el desarrollo de nuevas armas. A esto se suma la precariedad de los tratados vigentes para el control de la proliferación de armas de destrucción masiva y de sus vectores de lanzamiento.

La amenaza biológica, entendida como el empleo deliberado de agentes patógenos, toxinas o elementos genéticos u organismos genéticamente modificados dañinos por parte de Estados, individuos, redes criminales u organizaciones terroristas, supone una amenaza real con posibles consecuencias catastróficas.

El régimen de prohibición de armas químicas también se enfrenta a importantes retos, como los ataques registrados en los últimos años en Siria.

Asimismo, los riesgos derivados del desvío y contrabando de materiales de doble uso aumentan considerablemente debido a la transferencia de conocimiento tecnológico y el movimiento global de mercancías.

Efectos del cambio climático y de la degradación del medio natural

El cambio climático es una amenaza para la seguridad global y, en Europa, especialmente para el área mediterránea. Por eso la mitigación y adaptación al cambio climático adquieren cada vez más urgencia.

El cambio climático potencia las olas de calor, la reducción de los recursos hídricos, la desertificación y los fenómenos meteorológicos adversos. Ámbitos como la seguridad energética y la seguridad ambiental, en particular la gestión del agua, la biodiversidad, la calidad del aire, la despoblación de zonas agrarias o forestales se ven afectados por los efectos del cambio climático. Riesgos de origen natural relacionados con el clima, como son las inundaciones y los incendios forestales, tienen cada vez mayor incidencia en la seguridad, pues cada vez son más severos y frecuentes.

El deterioro del medio ambiente, de la biodiversidad y de sus servicios ecosistémicos dificultan el acceso a recursos básicos como el agua potable, amplifican conflictos existentes y son causa de desplazamientos forzosos de personas, además de generar inseguridad alimentaria.

CAPÍTULO 4

Un planeamiento estratégico integrado

Este capítulo establece los objetivos de la Estrategia y desarrolla un planeamiento integrado para la Política de Seguridad Nacional con una estructura diseñada con tres ejes estratégicos: Proteger, Promover y Participar.

La Estrategia de Seguridad Nacional establece tres objetivos:

El primer objetivo es avanzar en el modelo de gestión de crisis. Esto supone adoptar un enfoque anticipatorio y centrar la toma de decisiones en el análisis de hechos y datos objetivos. El Sistema de Seguridad Nacional enfocará sus esfuerzos en la alerta temprana, la formulación de medidas preventivas y la coordinación reforzada entre todos los entes públicos. Esto incluye un marco de cogobernanza con las Comunidades Autónomas en cuestiones donde las competencias son autonómicas o compartidas.

Para la gestión de crisis de carácter transnacional será necesario potenciar los procedimientos de actuación coordinada de la Unión Europea, a través de mecanismos de monitorización de riesgos y el desarrollo de bases de datos conjuntas para la identificación y valoración de potenciales riesgos y amenazas.

El segundo objetivo es favorecer la dimensión de seguridad de las capacidades tecnológicas y de los sectores estratégicos. Esto requiere incorporar aspectos de seguridad en el desarrollo tecnológico desde su concepción. Asimismo, implica constantes adaptaciones y actualizaciones que afectan al ámbito regulatorio, a los controles de calidad y a la formación.

El fomento de iniciativas y proyectos de I+D+i es fundamental para que, tanto desde los organismos públicos como desde el sector empresarial, se promueva el desarrollo tecnológico orientado a prevenir y a combatir los riesgos y las amenazas en sectores estratégicos, como la seguridad alimentaria, la salud o la ciberseguridad. En particular, es necesario tomar conciencia del potencial estratégico de la Inteligencia Artificial y la importancia de esta tecnología como puntal de la Seguridad Nacional.

El tercer objetivo es desarrollar la capacidad de prevención, disuasión, detección y respuesta de España frente a estrategias híbridas, en un contexto de seguridad en el que las amenazas convencionales se alternan con el uso combinado de vectores económicos, tecnológicos, diplomáticos y de información, entre otros, como elementos de presión y desestabilización.

La Estrategia establece tres ejes estratégicos sobre los que se articulan las líneas de acción (L.A.) de la política de Seguridad Nacional:

– Una España que protege la vida de las personas y sus derechos y libertades, así como el orden constitucional.
– Una España que promueve la prosperidad y el bienestar de los ciudadanos.
– Una España que participa en la preservación de la paz y la seguridad internacional y defiende sus intereses estratégicos.

Gran parte de las líneas de acción incorporan elementos de alineación o convergencia con medidas europeas e internacionales, reflejo de la naturaleza global de la mayoría de las amenazas a la Seguridad Nacional.

La cultura de Seguridad Nacional es un complemento importante para el desarrollo y la consolidación de la Política de Seguridad Nacional, ya que la concienciación social contribuye a fortalecer la resiliencia de la sociedad y del Estado. Para ello, es necesario implementar las acciones incluidas en el Plan Integral de Cultura de Seguridad Nacional, a través de la colaboración de las administraciones públicas, el sector privado y la sociedad civil, en cuatro ámbitos de actuación: formación; comunicación pública y divulgación; relevancia exterior; y participación activa de la ciudadanía y de las organizaciones de la sociedad civil.

Primer eje: Una España que protege la vida de las personas y sus derechos y libertades, así como el orden constitucional

El fortalecimiento de las capacidades de los componentes fundamentales de la Seguridad Nacional –la Defensa Nacional, la Acción Exterior y la Seguridad Pública, con el apoyo de los Servicios de Inteligencia e Información del Estado– junto al refuerzo de la Sanidad Pública, la Protección Civil y la protección de las Infraestructuras Críticas son claves para hacer frente a las amenazas que afectan a los valores e intereses de España y contribuyen a su cohesión territorial.

Disuasión y defensa

La protección de la soberanía nacional, la población y su libertad requiere disponer de unas adecuadas capacidades militares, tecnológicamente avanzadas, que contribuyan a garantizar una disuasión creíble, desde la premisa de que la diplomacia y el Derecho Internacional son los principales instrumentos para proteger los intereses nacionales.

Esta mejora de las capacidades militares asociadas a la disuasión y la defensa ha de ser sostenible en el largo plazo, lo que exige disponer de un marco presupuestario estable. Asimismo, demanda una política activa de colaboración público-privada que apoye firmemente al sector industrial y tecnológico de la seguridad y la defensa en España.

La adaptación al nuevo escenario estratégico requiere garantizar capacidades que cubran todo el espectro de la crisis o el conflicto, desde las operaciones de combate hasta el apoyo a autoridades civiles en la gestión de crisis.

España contribuirá a la capacidad de la OTAN para desarrollar tareas de defensa colectiva, de gestión de crisis y de respuesta a desastres y catástrofes, dentro de una visión global que incorpora todos los aspectos del conflicto y las operaciones. Además, trabajará para integrar los sistemas de mando y control nacionales con los internacionales, aliados, correspondientes.

Para la disuasión y la defensa:

L.A. 1. Asegurar las capacidades militares necesarias para proporcionar una disuasión creíble y una respuesta eficaz en todo el espectro de la crisis o conflicto, garantizando su sostenibilidad en el tiempo bajo un marco presupuestario, suficiente y estable.

L.A. 2. Reforzar las capacidades de defensa a través de la investigación, el desarrollo y la innovación tecnológica como vectores de ventaja estratégica.

L.A. 3. Desarrollar el sector industrial de la defensa, la seguridad y el espacio, así como las tecnologías duales, mediante la cooperación público-privada y el aprovechamiento de sinergias con las herramientas existentes tanto en el marco nacional como de las Organizaciones Internacionales de Seguridad y Defensa a las que pertenece España, en particular los Fondos Europeos de Defensa y la Cooperación Estructurada Permanente de la Unión Europea.

Lucha contra el terrorismo y la radicalización violenta

Para reducir la vulnerabilidad de la sociedad es necesario neutralizar la amenaza que representan las acciones terroristas dirigidas contra los ciudadanos y los intereses de España dentro y fuera de sus fronteras y hacer frente a los procesos de radicalización que conducen al extremismo violento.

Además del papel de las Fuerzas y Cuerpos de Seguridad y de los Servicios de Inteligencia, la participación de las Fuerzas Armadas en misiones internacionales contra el terrorismo resulta fundamental para hacer frente a esta amenaza, así como una actuación coordinada de todos estos actores.

Los principales vectores de la amenaza y en los que se deben concentrar los esfuerzos son los actores solitarios, los combatientes terroristas extranjeros, la propaganda yihadista y extremista y la radicalización en las prisiones. También es necesario participar en iniciativas internacionales cuyo objetivo es impedir que determinadas zonas puedan convertirse en refugio para terroristas, bien sea por la debilidad de los gobiernos de esos territorios o por la afinidad ideológica de estos con los grupos yihadistas.

La actuación en materia de lucha contra el terrorismo se estructura en cuatro pilares: prevenir, proteger, perseguir y preparar la respuesta, que sirven como base para el desarrollo de las principales medidas contra esta amenaza. Así lo establece la Estrategia Nacional contra el Terrorismo 2019, que es la principal referencia nacional en esta materia y consta de dos desarrollos fundamentales: el Plan Estratégico Nacional de Prevención y Lucha Contra la Radicalización Violenta 2020 y el Plan Estratégico Nacional de Lucha Contra la Financiación del Terrorismo 2020.

En relación con la radicalización, es fundamental reforzar la colaboración ciudadana, siendo prioritaria la constitución de las Oficinas de Prevención en las Delegaciones de Gobierno y de los grupos territoriales de prevención en las Juntas Locales de Seguridad. En el caso de aquellas Comunidades Autónomas que ya dispongan de programas específicos, la coordinación se llevará a cabo de acuerdo a su estructura y diseño.

Por otro lado, se requiere fomentar y actualizar las herramientas para la prevención, la detección y el seguimiento de los procesos de radicalización, en general, con la colaboración ciudadana y en los centros penitenciarios, en particular, con programas de tratamiento y evaluación del riesgo de radicalización.

Respecto a la financiación del terrorismo, el desarrollo de la interoperabilidad entre los sistemas existentes en las distintas instituciones permitirá identificar a los actores implicados y posibilitar la trazabilidad completa de los fondos que sean susceptibles de emplearse con fines terroristas.

Para atajar las actividades terroristas o de radicalización en la red y cumplir con la normativa europea, se creará la Unidad Nacional de Notificación de Contenidos de Internet para la monitorización y retirada de contenidos ilícitos de Internet.

Adicionalmente, se debe actualizar el plan de protección y prevención antiterrorista exterior centrado en la asistencia a los ciudadanos o activos españoles víctimas de ataques terroristas fuera de España.

Para la lucha contra el terrorismo y la radicalización violenta:

L.A. 4. Desarrollar herramientas y capacidades que refuercen la ejecución de investigaciones en el ámbito de la lucha contra el terrorismo por parte de los organismos implicados, así como reforzar la coordinación de esos organismos.

L.A. 5. Potenciar el desarrollo e implementación del Plan Estratégico Nacional de Prevención y Lucha Contra la Radicalización Violenta (PENCRAV) y del Plan Estratégico Nacional de Lucha Contra la Financiación del Terrorismo (PENCFIT).

L.A. 6. Incrementar la contribución española en iniciativas de ámbito internacional relativas al contraterrorismo y promover la capacitación y fortalecimiento de organismos e instituciones con competencias en contraterrorismo en países especialmente afectados.

L.A. 7. Potenciar las capacidades de prevención en la lucha contraterrorista de las actividades vinculadas al terrorismo y a extremismos violentos, especialmente en Internet y redes sociales.

L.A. 8. Actualizar el plan de protección y prevención antiterrorista en sus dimensiones interior y exterior.

Actuación frente a situaciones de crisis

Ante amenazas que trasciendan los marcos ordinarios de respuesta, la gestión de crisis del Sistema de Seguridad Nacional ha de contar, en primer lugar, con un sistema de información para el apoyo a la decisión basado en el análisis de indicadores que proporcione alerta temprana sobre los riesgos y amenazas a la Seguridad Nacional. En segundo lugar, requiere una red de comunicaciones segura, que permita integrar la información y ofrecer una respuesta desde una estructura de mando y control nacional. En tercer lugar, es necesario disponer de un catálogo actualizado de recursos humanos y materiales y de planes de preparación y disposición de estos para hacer frente a las situaciones de crisis. Todo ello, en un marco normativo actualizado de Seguridad Nacional.

Por otro lado, la dependencia del exterior en el suministro de recursos estratégicos supone una vulnerabilidad que se ha de paliar con una adecuada política industrial, tanto a nivel nacional como europeo, que apoye la capacidad de producción de recursos nacionales.

Entre las medidas de carácter sectorial, la lucha contra las epidemias y pandemias demanda la modernización del sistema de vigilancia epidemiológica nacional, a partir de las lecciones aprendidas en la gestión de la pandemia de la COVID-19. Es necesario actualizar el sistema de vigilancia nacional de Salud Pública para permitir una respuesta ágil y acertada.

En el Sistema Nacional de Protección Civil, la consolidación de estructuras funcionales y redes de coordinación, junto con la asignación de los recursos necesarios, contribuirán a fortalecer la gestión de emergencias y catástrofes, de acuerdo con lo establecido en el Plan Estatal General de Emergencias de Protección Civil. Asimismo, es importante asegurar el intercambio de información permanente y en tiempo real entre el Sistema Nacional de Protección Civil y el Sistema de Seguridad Nacional en caso de catástrofe.

Las Infraestructuras Críticas constituyen el eje sobre el que se articula la resiliencia física de un país. Incluyen los sectores de la salud, energético, de alimentación, de transportes y el suministro de agua entre otros. Su funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.

Es preciso impulsar la dimensión preventiva del Sistema Nacional de Protección de las Infraestructuras Críticas, con especial énfasis en la protección de los sistemas informáticos de las Infraestructuras Críticas y operadores de servicios esenciales frente a ciberamenazas. En este sentido, la colaboración público-privada y el I+D+i para robustecer la resiliencia frente a ciberataques es clave.

Las Ciudades Autónomas de Ceuta y Melilla, por su localización geográfica en el continente africano y por la especificidad de su frontera española y europea, requieren de una especial atención por parte de la Administración General del Estado para garantizar la seguridad y el bienestar de sus ciudadanos.

Para hacer frente a situaciones de crisis:

L.A. 9. Desarrollar el modelo de gestión integral de crisis en el Sistema de Seguridad Nacional a través de la elaboración de un reglamento de gestión de crisis; la implantación de un sistema de alerta temprana basado en indicadores; la creación de un catálogo de recursos y de planes de preparación y disposición de recursos; y el diseño de un Plan de ejercicios de preparación en el marco de la Seguridad Nacional.

L.A.10. Crear la Reserva Estratégica basada en capacidades nacionales de producción industrial con una triple orientación:

a) Identificar los recursos industriales esenciales de las diferentes Administraciones Públicas y del sector privado correspondientes a sus respectivos ámbitos competenciales.

b) Garantizar el suministro de aquellos bienes y servicios que sean considerados como de primera necesidad y carácter estratégico.

c) Salvaguardar la base industrial que suministra recursos de primera necesidad y carácter estratégico, como pudieran ser componentes electrónicos, materiales estratégicos, maquinaria de alta tecnología, aeronáutica, semiconductores, química esencial, equipos agrarios avanzados, tecnología de la comunicación o equipos sanitarios, entre otros.

L.A. 11. Modernizar el sistema de vigilancia nacional de Salud Pública a través de la renovación de las tecnologías sanitarias y los sistemas de información. La Estrategia Digital del Servicio Nacional de Salud incluirá medidas para mejorar la prevención, el diagnóstico, la vigilancia y la gestión de la salud en un marco de cogobernanza con las Comunidades Autónomas.

L.A. 12. Elaborar un Plan Integral de Seguridad para Ceuta y Melilla.

Contrainteligencia, lucha contra las campañas de desinformación y acción frente a las injerencias del exterior

Para proteger los intereses de España se debe prevenir, detectar y neutralizar las agresiones encubiertas procedentes del exterior, cuyo objetivo es obtener información sensible de forma ilegal para atacar la imagen internacional de España o realizar acciones de injerencia.

Esto incluye reforzar e integrar las capacidades de los Servicios de Inteligencia para hacer frente a las operaciones en el ciberespacio y al espionaje, amenazas que cada vez cobran mayor relevancia por su capacidad de desestabilizar las instituciones del Estado y por su impacto sobre la vida y libertad de los ciudadanos. Para ello, resulta necesario que los Servicios de Inteligencia españoles se mantengan al nivel de los más relevantes de la Unión Europea. En este sentido, se potenciarán sus capacidades humanas y tecnológicas, de manera que se sigan aprovechando las ventajas vinculadas a una adecuada gestión y tratamiento del dato, como la Inteligencia Artificial la computación cuántica o la nube. Además, se velará por la adecuada actualización legislativa para garantizar tanto los derechos de los ciudadanos españoles, como la capacidad de los Servicios de actuar en su defensa.

La protección del patrimonio científico y tecnológico requerirá un esfuerzo adicional por parte del Centro Nacional de Inteligencia (CNI), del Centro Criptológico Nacional (CCN) y de la Oficina Nacional de Seguridad (ONS). En este sentido, será esencial un creciente esfuerzo en las actividades de sensibilización frente a las actuaciones de Servicios de Inteligencia hostiles en el ámbito de la industria nacional y de los sectores estratégicos. Asimismo, el refuerzo de la ONS será fundamental, en línea con la creciente importancia de la protección de la información clasificada como recurso esencial para la Seguridad Nacional. Medida que, a su vez, favorecerá la participación de la industria española en programas clasificados en el exterior.

Por otro lado, hacer frente a las campañas de desinformación, que socavan la confianza a de los ciudadanos en las instituciones democráticas y conducen a la polarización social, requiere hacer un uso sistemático de la detección, alerta temprana y notificación así como la coordinación de la respuesta, siempre en línea con las pautas y el trabajo desarrollado en el seno de la Unión Europea. La colaboración público-privada, especialmente con los medios de comunicación y proveedores de redes sociales, y la sensibilización de la ciudadanía son aspectos clave a la hora de detectar y hacer frente a las campañas de desinformación.

Las iniciativas nacionales estarán coordinadas con los planes existentes a nivel europeo, como el Plan de Acción contra la Desinformación y el Plan de Acción para la Democracia Europea.

Para la Contrainteligencia, lucha contra las campañas de desinformación y acción frente a las injerencias del exterior:

L.A. 13. Elaborar una Estrategia Nacional de Lucha contra las campañas de desinformación.

L.A. 14. Incrementar las capacidades de los Servicios de Inteligencia españoles frente a los ataques de los Servicios de Inteligencia hostiles, en especial en el ciberespacio.

L.A. 15. Potenciar las capacidades de la Oficina Nacional de Seguridad y garantizar un marco legal adecuado para la protección de la información clasificada.

L.A. 16. Reforzar la cooperación internacional en materia de contrainteligencia.

Segundo eje: Una España que promueve la prosperidad y el bienestar de los ciudadanos

En un contexto marcado por la necesidad de recuperación económica, el crecimiento inclusivo y la creación de empleo requieren políticas de inversión en innovación y competitividad con visión de futuro, de manera que contribuyan a reforzar la resiliencia de la sociedad a largo plazo.

Seguridad de los espacios comunes globales

El normal desarrollo de la actividad social y económica depende, en gran medida, de la libre circulación de personas, bienes, servicios e ideas que se realizan a través de los espacios comunes globales: el ciberespacio, el espacio marítimo y el espacio aéreo y ultraterrestre.

Son espacios de conexión caracterizados por su apertura funcional, la carencia de fronteras físicas y su fácil accesibilidad. Por otro lado, en los espacios comunes globales resulta difícil la atribución de cualquier acción irregular o delictiva, dada su extensión, su débil regulación y la ausencia de soberanía.

Ciberespacio:

En términos de ciberseguridad, se requiere garantizar el uso seguro y fiable del ciberespacio, para proteger los derechos y las libertades de los ciudadanos y promover el progreso socio económico. Para ello es importante incrementar las capacidades (tecnológicas, humanas y económicas) de la ciberseguridad nacional dirigidas a la prevención, detección, respuesta, recuperación, investigación y defensa activa.

La Carta de Derechos Digitales supone un paso adelante en la protección de los derechos de la ciudadanía en el entorno virtual actual. Esto incluye el reconocimiento del derecho a la igualdad en los ámbitos digitales, la no discriminación y la no exclusión.

En la Administración pública, es ineludible avanzar en el modelo de gobernanza de la ciberseguridad nacional, sobre la base de una mayor eficiencia en los recursos y la integración de las capacidades nacionales. En este sentido, el Centro de Operaciones de Ciberseguridad permitirá, mediante la prestación de servicios horizontales, aumentar las capacidades de vigilancia, detección y respuesta ante ciberataques contra la Administración General del Estado y sus organismos públicos, así como contra las administraciones autonómicas y locales. Un aspecto relevante será el desarrollo de las infraestructuras de ciberseguridad en las Comunidades y Ciudades Autónomas.

Prioridades adicionales son la creación de un sistema de observación y medición de la situación de la ciberseguridad nacional y la puesta en marcha de una plataforma nacional de notificación y seguimiento de ciberincidentes que permita medir el intercambio de información entre organismos públicos y privados en tiempo real.

Por otro lado, será preciso implementar los nuevos requerimientos previstos en el marco de la Unión Europea en la Estrategia de Ciberseguridad de la UE para la Era Digital y en la adecuación de las nuevas propuestas normativas, que han de incluir la legislación necesaria para la protección de las redes y sistemas.

Espacio marítimo:

La Estrategia de Seguridad Marítima promueve un enfoque integral que potencie la actuación coordinada y cooperativa de las diferentes Administraciones; la adopción de medidas para fortalecer la capacidad de actuación del Estado en la mar y en su litoral; el impulso de la colaboración con el sector privado; y, por último, el fomento de la cooperación internacional, en particular a través de la aplicación de las iniciativas de la Organización Marítima Internacional, la Estrategia de Seguridad Marítima de la Unión Europea y la Estrategia Marítima de la OTAN.

Una de las prioridades en el ámbito marítimo es la seguridad de la flota mercante y pesquera española en aguas jurisdiccionales e internacionales.

Además, en el marco de la Seguridad Nacional, es indispensable una planificación preventiva que proporcione respuestas efectivas ante situaciones de complejidad que requieran una actuación concertada de los diversos organismos implicados en el dominio marítimo. Esto supone introducir tecnologías de Inteligencia Artificial en sistemas, plataformas y sensores de vigilancia marítima para la modernización de las capacidades marítimas.

Espacio aéreo y ultraterrestre:

Es esencial garantizar la seguridad del espacio aéreo y ultraterrestre en un marco compartido y orientado a prevenir los riesgos y amenazas que en ellos se desarrollan, así como neutralizar sus consecuencias, conforme a los principios de eficiencia y máxima coordinación, tanto en el empleo de las capacidades de análisis y evaluación como en las de respuesta ante los riesgos y las amenazas.

La seguridad frente a la amenaza de vehículos aéreos no tripulados precisa de acciones urgentes, dada su proliferación.

El sector espacial es clave para la Seguridad Nacional por los servicios que proporciona. Es preciso desarrollar una política de seguridad en el espacio ultraterrestre basada en la cooperación internacional, que tenga como eje la colaboración entre todos los actores implicados. En este sentido, España debe incorporarse a todas aquellas iniciativas internacionales orientadas a preservar el uso pacífico del espacio ultraterrestre, con especial atención a los programas espaciales de la Unión Europea.

Ante la evolución acelerada del sector, debe alcanzarse un reparto eficaz y eficiente de competencias espaciales entre los diversos organismos involucrados. La creación de una Agencia Espacial Española contribuirá a ordenar las competencias y establecer una política nacional que sirva de guía, tanto al sector público como al privado. Así, se podrá maximizar el rendimiento de las inversiones, fomentar espacios de colaboración públicos y privados, facilitar el uso dual de las capacidades espaciales y potenciar el sector de la industria espacial nacional de forma clara y coherente. Además, la Agencia representará internacionalmente a España en el sector espacial.

Para la seguridad de los espacios comunes globales:

En el ciberespacio:

L.A.17. Avanzar en la integración del modelo de gobernanza de la ciberseguridad en el marco del Sistema de Seguridad Nacional.

En el espacio marítimo:

L.A. 18. Elaborar escenarios de riesgo y planes de preparación y respuesta para aquellas situaciones que se consideren de especial interés para la Seguridad Nacional en el ámbito de la seguridad marítima.

En el espacio aéreo y ultraterrestre:

L.A. 19. Crear la Agencia Espacial Española, con un componente dedicado a la Seguridad Nacional, para dirigir el esfuerzo en materia espacial, coordinar de forma eficiente los distintos organismos nacionales con responsabilidades en el sector espacial y unificar la colaboración y coordinación internacional.

Estabilidad económica y financiera

Un contexto económico justo, estable y seguro es condición necesaria para el progreso y favorece la creación de empleo, así como la competitividad de las empresas y la industria española.

La estrategia económica para hacer frente a la crisis derivada de la pandemia está recogida en el Plan de Recuperación, Transformación y Resiliencia. Este Plan traza la hoja de ruta para la modernización de la economía española, la recuperación del crecimiento económico y la creación de empleo tras la crisis de la COVID-19, así como para responder a los retos de la próxima década.

Las medidas que se adopten han de ir acompañadas de una política fiscal robusta y progresiva de acuerdo con el principio de estabilidad presupuestaria y sostenibilidad financiera y que promueva medidas contra la evasión de impuestos, el blanqueo de capitales y la corrupción.

Asimismo, para ejecutar una política preventiva y anticipar posibles crisis, es importante monitorizar los riesgos sistémicos y la publicación de alertas sobre aspectos que puedan afectar a la estabilidad financiera.

Por otra parte, la sostenibilidad del crecimiento económico a medio plazo requiere impulsar la modernización y la productividad del ecosistema industrial español. Este aspecto cobra también sentido en relación a determinados activos estratégicos para la Seguridad Nacional que son objeto de inversión directa extranjera. La tecnología, la salud, el sector aeroespacial o las energías renovables, área esta última en la que España ocupa una posición de liderazgo, son sectores industriales estratégicos para la seguridad. Se han de potenciar, desde una economía abierta, en línea con el marco normativo europeo y el mecanismo de coordinación de la Unión Europea, pero también con vistas a asegurar la cadena de valor, contribuir a una mayor autonomía estratégica y, por tanto, a una mayor resiliencia en situaciones de crisis.

Para la estabilidad económica y financiera:

L.A. 20. Potenciar la modernización y la productividad del ecosistema español industrial, mediante el impulso de la competitividad de sectores estratégicos clave para la Seguridad Nacional, en línea con lo establecido en el Plan de Recuperación, Transformación y Resiliencia.

Lucha contra el crimen organizado y la delincuencia grave

Las políticas públicas contra la criminalidad organizada y la delincuencia grave deben orientarse hacia la identificación temprana de la actividad delictiva, su prevención, persecución y represión efectivas. Para ello, se debe promover la actuación coordinada de los Servicios de Inteligencia, Fuerzas y Cuerpos de Seguridad y autoridades fiscal y judicial. A la lucha directa contra la criminalidad desde las instituciones públicas, debe sumarse además la concienciación social sobre el fenómeno delictivo. En este sentido, en marzo de 2020 se aprobó el Plan Estratégico contra la Criminalidad.

Para neutralizar la economía del crimen organizado, se necesitan instrumentos que mejoren la inteligencia y la detección, además de nuevas capacidades de ciberseguridad. Para ello, hay que establecer un plan estratégico que incluya el blanqueo de capitales y la recuperación y localización de activos.

El desarrollo de un plan contra la trata y la explotación de seres humanos, especialmente de mujeres y niñas, contribuirá a hacer frente a las desigualdades sociales que genera la criminalidad y a la situación de vulnerabilidad en la que se encuentran ciertos colectivos respecto a los delitos de odio.

Además, es indispensable establecer planes específicos de actuación contra el crimen organizado en las áreas geográficas especialmente proclives a su implantación, actuación y arraigo, como se ha hecho con el plan para el Estrecho de Gibraltar.

Por otro lado, se requiere impulsar nuevas vías de prevención, investigación y análisis de la vinculación entre el crimen organizado y el terrorismo.

Para la lucha contra el crimen organizado y la delincuencia grave:

L.A. 21. Elaborar un plan estratégico de lucha contra el enriquecimiento ilícito de las organizaciones criminales y los delincuentes.

L.A. 22. Desarrollar un plan estratégico específico nacional contra la trata y la explotación de seres humanos.

Ordenación de flujos migratorios

La ordenación de los flujos migratorios y la lucha contra las redes de migración irregular y trata de seres humanos deben ser elementos de permanente atención por parte de las Administraciones Públicas, con la implicación del tercer sector y la sociedad civil.

La articulación de mecanismos que mejoren la eficiencia y la integración de todos los esfuerzos y las capacidades de las Administraciones Públicas redundará en una mayor eficacia y coherencia en la gestión migratoria.

Desde una perspectiva integral y preventiva, la colaboración con los países de origen y tránsito es un aspecto indispensable e insustituible para reducir los movimientos migratorios irregulares hacia España. Por ello, resulta esencial reforzar y aumentar los convenios de colaboración en el ámbito bilateral y en el marco de la Unión Europea, en especial en el Magreb, Sahel y África occidental. Además, establecer nuevas vías de migración regular y mejorar las existentes es una parte esencial del compromiso con los países africanos.

La vigilancia y el control de las fronteras es un elemento fundamental en este ámbito. Por un lado, es una responsabilidad compartida, incluidos los países de origen y tránsito, a los que se debe asistir para incrementar sus capacidades y medios. Por otro lado, en cuanto las fronteras exteriores de la Unión Europea, la inmigración irregular es una responsabilidad no solo de los países frontera de la Unión, sino que concierne a todos los socios europeos. Además de las rutas marítimas y terrestres, es imperativo atender a las llegadas aéreas, tanto desde África como desde otros continentes, a los movimientos secundarios hacia o desde España y a la prolongación ilegal de estancia que deriva en inmigración irregular.

Igualmente, es importante la identificación temprana de grupos vulnerables, así como de eventuales beneficiarios de protección internacional, y la mejora de los centros adecuados para su atención.

La optimización de las capacidades de salvamento y rescate en la mar, la atención humanitaria, la recepción y reseña y el tratamiento de los inmigrantes durante todo el ciclo migratorio, incluidos los procesos de determinación de estatus de los solicitantes de protección internacional, requieren actualizar la legislación nacional.

La inclusión de los migrantes es un vector fundamental para lograr una sociedad más próspera, cohesionada y resiliente. Para la consecución de este objetivo, es imprescindible mejorar la coordinación entre los tres niveles de la Administración General del Estado y establecer políticas públicas dirigidas a erradicar cualquier forma de discriminación, racismo o xenofobia.

Para la ordenación de flujos migratorios:

L.A. 23. Establecer un sistema integral y colaborativo de información a nivel de la Administración General del Estado, que permita conocer en tiempo oportuno la situación de los flujos de inmigración, los recursos comprometidos en su gestión, así como las necesidades identificadas.

L.A. 24. Fortalecer la relación y los acuerdos con los países de origen y tránsito para lograr una migración ordenada e impedir el tráfico de seres humanos.

Seguridad energética y transición ecológica

La transición energética hacia un modelo más sostenible, que incorpore un mayor porcentaje de energías renovables y contribuya a lograr la neutralidad climática y una mayor autonomía estratégica, introduce nuevas oportunidades y retos en el escenario energético, que se suman a la necesidad de garantizar la seguridad del abastecimiento y transporte de hidrocarburos en los próximos años.

Las energías renovables y las infraestructuras del sistema energético, en particular las redes eléctricas que las transportan, tienen repercusiones geopolíticas propias. Así, las tecnologías asociadas a la transición energética, las instalaciones y los nuevos materiales, como las tierras raras, están ganando protagonismo frente a recursos más tradicionales como el petróleo y el gas.

Los cambios en la matriz energética conllevan la incorporación de nuevas tecnologías y, en consecuencia, la ampliación y/o profundización de la dependencia de las mismas.

El nuevo paradigma energético obliga a una revisión de la Estrategia de Seguridad Energética Nacional 2015, para una adecuada actualización y encaje en este marco, donde además se han de tener en consideración el Pacto Verde Europeo y los Acuerdos de París de 2015.

El Plan Nacional de Adaptación al Cambio Climático 2021-2030 es el instrumento de planificación básico para promover la acción coordinada y coherente entre departamentos ministeriales, Comunidades Autónomas y entes locales.

Para la seguridad energética y transición ecológica:

L.A. 25. Actualizar la Estrategia de Seguridad Energética Nacional para establecer objetivos y líneas de acción de acuerdo con el contexto de transición ecológica, energética y económica.

Tercer eje: Una España que participa en la preservación de la paz y seguridad internacional y defiende sus intereses estratégicos

España es firme defensora del respeto y cumplimiento del Derecho Internacional. Al mismo tiempo, reconoce la necesidad de algunas reformas del sistema internacional. En particular, aboga por una revisión del sistema de las Naciones Unidas, eje central de la acción multilateral concertada para la prevención de conflictos, la acción humanitaria y la consecución de la paz, para lograr una organización más ágil y eficaz, adaptada a los desafíos mundiales actuales.

Asimismo, los mecanismos de gobernanza global son oportunos para gestionar bienes públicos como la salud pública, la seguridad y sanidad alimentaria o el medioambiente.

Un enfoque preventivo y cooperativo de la seguridad es el principal criterio del compromiso de España con la comunidad internacional. Además, España promueve un enfoque integral en la resolución de conflictos en el exterior, basado en una cooperación multidimensional que fortalezca la gobernanza, la seguridad y el progreso.

España incorpora la igualdad de género como un elemento distintivo de su acción exterior, así como el cumplimiento de la Agenda Mujeres, Paz y Seguridad, con el objetivo de avanzar hacia la igualdad real y efectiva en el plano internacional.

Multilateralismo reforzado

España es un país comprometido con la paz y seguridad internacional. Ningún país por sí solo puede hacer frente a amenazas globales del siglo XXI como la lucha contra las pandemias o contra los efectos del cambio climático. Una acción concertada sobre la base de un multilateralismo más fuerte resulta necesaria con la Organización de Naciones Unidas como principal referencia a nivel mundial. Las iniciativas orientadas a que la Organización Mundial de la Salud sea un instrumento más eficaz forman parte de la propuesta española. Además, se ha de impulsar un control de armamentos que responda al mundo multipolar e incorpore a China.

Para el multilateralismo reforzado:

L.A. 26. Potenciar la diplomacia preventiva y el papel de España como actor activo y comprometido en la mediación de conflictos en el exterior.

L.A. 27. Contribuir a la intensificación del apoyo al régimen internacional de no proliferación de armas de destrucción masiva y desarme, a través de la actualización de el régimen internacional de control, exportación y verificación.

L.A. 28. Impulsar la implementación de los objetivos del II Plan Nacional de Acción de Mujeres, Paz y Seguridad de integrar la perspectiva de género y hacer realidad la participación significativa de las mujeres en la prevención, gestión y resolución de conflictos y la consolidación de la paz.

Autonomía estratégica europea

La autonomía estratégica implica un mayor peso geopolítico de la Unión Europea en la esfera mundial, que puede ser utilizado para equilibrar asimetrías de influencia entre grandes actores, promover una gobernanza justa frente a retos globales como el desarrollo tecnológico, el cambio climático o la lucha contra las pandemias y defender sus valores e intereses.

La autonomía estratégica trasciende el ámbito de la defensa. La construcción del marco europeo de la seguridad sanitaria, las acciones para aumentar la resiliencia de las cadenas de suministro, el avance en la seguridad energética o el impulso hacia una soberanía tecnológica forman parte, entre otros, del amplio espectro de políticas tendentes al fortalecimiento de la seguridad europea y del papel de la Unión como actor global. En este sentido, es clave la reducción de las dependencias estratégicas de materias primas y componentes esenciales de las cadenas de valor industriales, a través de la diversificación de la producción y el suministro, el mantenimiento de reservas y el impulso a la producción e inversión en Europa.

Un pilar esencial de la seguridad europea es ahondar en la complementariedad entre la Unión Europea y la OTAN. Una Europa con mayores capacidades contribuye a una Alianza Atlántica más fuerte y viceversa. La asunción por parte de los aliados europeos de una mayor cuota de responsabilidad en materia de seguridad y defensa refuerza el compromiso asumido.

Otro aspecto relevante es el desarrollo de una mayor cooperación policial, militar, de inteligencia y judicial en la Unión Europea para luchar contra el terrorismo, el crimen organizado y la delincuencia grave.

Para la autonomía estratégica europea:

L.A. 29. Promover un liderazgo decidido en la formulación y el desarrollo de la Política Común de Seguridad y Defensa, en línea con las conclusiones que se obtengan del proceso de revisión de la seguridad europea.

L.A. 30. Contribuir a reforzar las capacidades estratégicas autónomas de la Unión Europea, incluida la construcción de la Europa de la Defensa y el desarrollo de capacidades industriales y tecnológicas europeas.

Mayor protagonismo en la OTAN

La defensa colectiva es un elemento central para la Seguridad Nacional. El compromiso de España con el multilateralismo como mejor vía para proteger intereses y valores frente a las amenazas compartidas a la seguridad encuentra su mejor garantía en la participación

española en la OTAN. Una visión integral de los riesgos y amenazas a la seguridad, que incorpore los desafíos que presenta el flanco sur, ha de tener su debido reflejo en la reflexión estratégica que está acometiendo la Organización.

Para un mayor protagonismo en la OTAN:

L.A. 31. Participar activamente en la revisión estratégica acometida por la OTAN de acuerdo a las siguientes acciones:

a) Promover una mayor convergencia con la Unión Europea en políticas tecnológicas.

b) Enfatizar la importancia del flanco Sur, particularmente del Sahel, para la seguridad europea y transatlántica.

c) Mantener la contribución española a las operaciones OTAN en Europa oriental y al sistema de defensa antimisiles como vector de disuasión.

Preservación del medio ambiente, desarrollo sostenible y lucha contra el cambio climático

Los efectos del cambio climático son una de las amenazas más acuciantes para la Seguridad Nacional por su impacto transversal en ámbitos tan heterogéneos como la seguridad energética, las emergencias y catástrofes o los conflictos y desplazamientos de personas a consecuencia de la degradación medioambiental y los desastres naturales.

En particular, un importante nexo con la seguridad se encuentra en los posibles conflictos derivados de los efectos del cambio climático en los países más vulnerables. Por ello, en el Plan Nacional de Adaptación al Cambio Climático se aboga por políticas preventivas de ayuda al desarrollo, que pongan el foco en la construcción de la resiliencia a través de la detección temprana. A tal fin resulta necesaria la identificación de los lugares más vulnerables al cambio climático para priorizar la acción.

Los compromisos adquiridos en los Acuerdos de París de 2015 y la Agenda 2030 encuentran en el Plan Nacional de Acción para la implementación de la Agenda 2030 la principal referencia para avanzar en la lucha contra la crisis climática.

Para la preservación del medio ambiente, el desarrollo sostenible y la lucha contra el cambio climático:

L.A. 32. Integrar la Agenda 2030 en las políticas de cooperación al desarrollo, para contribuir a reforzar las capacidades de los países más vulnerables a prepararse frente al cambio climático.

L.A. 33. Desarrollar los objetivos del área «paz, seguridad y cohesión social» del Plan Nacional de Adaptación al Cambio Climático 2021-2030 relacionados con la prevención de posibles conflictos mediante su detección temprana, con el fin de reconocer aquellas situaciones que puedan suponer amenazas para la paz y la seguridad internacional.

CAPÍTULO 5

El Sistema de Seguridad Nacional y la Gestión de Crisis

El quinto capítulo de la Estrategia presenta un modelo integrado para hacer frente a las situaciones de crisis de forma preventiva, ágil y eficaz en el marco del Sistema de Seguridad Nacional.

El Sistema de Seguridad Nacional es el conjunto de órganos, organismos, recursos y procedimientos que posibilitan la acción del Estado en el ejercicio de las funciones para proteger la libertad y el bienestar de sus ciudadanos, garantizar la defensa de España y sus principios y valores constitucionales, y contribuir junto a socios y aliados a la seguridad internacional.

El Consejo de Seguridad Nacional es la pieza angular del Sistema y es el órgano responsable de la dirección y la coordinación de las actuaciones para la gestión de situaciones de crisis. Estas actuaciones están dirigidas a:

– Detectar y valorar los riesgos y amenazas concretos para la Seguridad Nacional.

– Facilitar el proceso de toma de decisiones.

– Asegurar una respuesta óptima y coordinada de los recursos del Estado que sean necesarios.

Para llevarlas a cabo, el Consejo de Seguridad Nacional está asistido por un Comité Especializado de carácter único para el conjunto del Sistema: el Comité de Situación.

El Comité de Situación estará apoyado por el resto de comités especializados, en sus respectivos ámbitos sectoriales, en todo lo relacionado con la valoración de riesgos y amenazas, en el análisis de los posibles escenarios de crisis, en especial de aquellos susceptibles de derivar en una situación de interés para la Seguridad Nacional, y en la evaluación de los resultados.

Un modelo avanzado de Gestión de Crisis

En un entorno de seguridad caracterizado por su elevada complejidad y un ritmo acelerado de cambio, se incrementa la probabilidad de que se produzcan eventos de difícil previsión y de gran impacto para la seguridad. Su prevención y gestión demandan instrumentos de detección y alerta temprana capaces de integrar y analizar toda la información disponible.

Enfoque integral que garantice la resiliencia

Un enfoque integral basado en la resiliencia cubre todas las fases de la gestión de crisis, desde un estado de normalidad hasta la recuperación tras una situación de crisis. Esta aproximación implica implementar estructuras y procesos ágiles que permitan la adopción de políticas anticipatorias, con la ayuda de la digitalización del sistema.

Además, el concepto de resiliencia supone una integración multinivel en el modelo de gestión de crisis, que incorpora tanto la coordinación entre todas las Administraciones públicas (estatal, autonómica y local), como entre los ministerios, el sector privado y científico y la sociedad civil.

A estos fines, y alineado con desarrollos similares en la Unión Europea y la OTAN, el Comité de Situación garantizará, en el marco de la gestión de crisis, el enfoque integral gubernamental y social para aumentar la capacidad de resiliencia frente a todo el espectro de los riesgos y las amenazas a la Seguridad Nacional, con especial atención a las estrategias híbridas, dado el carácter multidimensional y coordinado de este tipo de amenazas, que persiguen atentar contra la estabilidad de los Estados y las instituciones.

Estructuras y procesos

En el marco del Sistema de Seguridad Nacional, la dirección y coordinación de la gestión de crisis es función del Consejo de Seguridad Nacional, asistido por el Comité de Situación.

El Departamento de Seguridad Nacional apoya al Comité de Situación mediante la integración y el análisis de información procedente de todas las autoridades y organismos, la alerta temprana, el seguimiento de la situación y el asesoramiento técnico preventivo y las acciones de respuesta. Este apoyo se materializará a través de los mecanismos de enlace y coordinación del Sistema de Seguridad Nacional, tanto de carácter permanente como de coordinación reforzada. Así, se podrá activar una célula de coordinación, formada por representantes de todos los ministerios y organismos implicados en la respuesta y conducción de la crisis.

Además, el Departamento de Seguridad Nacional se constituye como punto de entrada y relación con los sistemas de gestión de crisis a nivel político-estratégico de la Unión Europea (Dispositivo de Respuesta Política Integrada a las Crisis) y de la OTAN, salvo en lo relativo a las implicaciones de la Defensa Nacional o en materia de Protección Civil.

A los efectos de una adecuada preparación y adiestramiento, conviene realizar ejercicios de gestión de crisis en el plano político-estratégico con carácter periódico. Estos ejercicios tendrán como objetivo general activar la estructura y los procedimientos del Sistema de Seguridad Nacional, ejercitando la gestión de crisis ante una situación de interés para la Seguridad Nacional.

Asimismo, los miembros del Sistema de Seguridad Nacional participarán en los ejercicios de las organizaciones internacionales cuando así sea preciso.

Desarrollo del Sistema

Para el desarrollo de capacidades nacionales para hacer frente a situaciones de crisis, se acometerán las siguientes iniciativas:

– Catálogo de recursos de la Seguridad Nacional. Se elaborará un catálogo dinámico de recursos de los sectores estratégicos del Estado que puedan ser puestos a disposición de las autoridades competentes. En su elaboración participará tanto el sector público como el privado.

A dichos efectos, las Comunidades Autónomas elaborarán sus catálogos específicos de recursos, que se integrarán en el estatal, sobre la base de sus propias competencias y la información facilitada por el Gobierno.

– Planes de preparación y disposición de recursos. Se elaborarán para aquellos escenarios aprobados por el Consejo de Seguridad Nacional que, en base al análisis de los riesgos y las amenazas, así lo aconsejen.

– Sistema de Alerta Temprana basado en indicadores. El modelo integrado para hacer frente a las situaciones de crisis, de forma preventiva, ágil y eficaz, está basado en un sistema que permita la toma de decisiones sobre la base de la información proporcionada por unos datos objetivos de determinación de impactos y la evidencia científica. A tales efectos, se desarrollará un sistema de indicadores críticos de los distintos ámbitos de la Seguridad Nacional, cuya monitorización y análisis permitan desplegar acciones preventivas y, llegado el caso, la ejecución de medidas de respuesta y conducción en tiempo oportuno.

– Integración de la información de Seguridad Nacional. Se adoptarán soluciones tecnológicas basadas en la gestión del conocimiento, y también, con técnicas de Inteligencia Artificial, para la evaluación de la situación de seguridad y el apoyo al análisis estratégico. Estos desarrollos permitirán la integración y el análisis de toda la información relevante, su distribución y puesta a disposición de todos los actores intervinientes en la gestión de la crisis, así como la interoperabilidad de los sistemas involucrados.

– Desarrollo de las comunicaciones especiales de la Presidencia del Gobierno. A través de las comunicaciones especiales, se establecerá un instrumento de gestión para el Sistema de Seguridad Nacional, que se configura como elemento de coordinación y para el intercambio de información clasificada en materia de gestión de crisis.

– Integración de las Comunidades y Ciudades Autónomas en el Sistema de Seguridad Nacional. Corresponde a la Conferencia Sectorial para asuntos de la Seguridad Nacional asumir las funciones como órgano de cooperación entre el Estado y las Comunidades Autónomas en aquellas cuestiones de interés común relacionadas con la Seguridad Nacional.

El acceso a las comunicaciones especiales de la Presidencia del Gobierno de todos los actores intervinientes en una situación de crisis es un requisito imprescindible para su integración efectiva en el Sistema de Seguridad Nacional. De esta forma, en los próximos cinco años se desarrollará un plan de extensión progresiva de esta red.

§ 21

Orden ISM/1320/2024, de 18 de noviembre, por la que se aprueba la Política de Seguridad de la Información del Ministerio de Inclusión, Seguridad Social y Migraciones y se crea el Comité de Seguridad de los Sistemas de Información

Ministerio de Inclusión, Seguridad Social y Migraciones
«BOE» núm. 283, de 23 de noviembre de 2024
Última modificación: sin modificaciones
Referencia: BOE-A-2024-24452

El marco de relación entre la Administración Pública y la ciudadanía a través de los medios electrónicos se encuentra establecido en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Por su parte, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, define en su artículo 156 el objeto del Esquema Nacional de Seguridad y lo incorpora como parte esencial en la configuración del archivo electrónico de los documentos regulado en el artículo 46 y en el régimen de relaciones electrónicas y transferencias de tecnología entre las Administraciones Públicas, tal como establece su artículo 158.

Ambas normas han sido objeto de desarrollo en virtud del Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.

La Administración Digital debe ser confiable para que la ciudadanía realice los trámites administrativos correspondientes con total seguridad y fiabilidad. Para ello, el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, persigue fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar a conocimiento de personas no autorizadas. El fundamento jurídico de esta orden se encuentra en el artículo 12 del mismo, que establece que cada administración pública contará con una política de seguridad formalmente aprobada por el órgano competente, y, en el caso de la Administración General del Estado, cada ministerio contará con su política de seguridad, que aprobará la persona titular del departamento, lo que enlaza con los principios de necesidad, seguridad jurídica y transparencia.

El Real Decreto 829/2023, de 20 de noviembre, por el que se reestructuran los departamentos ministeriales, atribuye en su artículo 21 al Ministerio de Inclusión, Seguridad Social y Migraciones la propuesta y ejecución de la política del Gobierno en materia de Seguridad Social y clases pasivas, así como la elaboración y el desarrollo de la política del Gobierno en materia de extranjería, inmigración y emigración y de políticas de inclusión. Con posterioridad, el Real Decreto 1009/2023, de 5 de diciembre, por el que se establece la estructura orgánica básica de los departamentos ministeriales, estableció en su artículo 20 la estructura del Ministerio de Inclusión, Seguridad Social y Migraciones hasta el nivel orgánico

de dirección general. Recientemente, se ha determinado la estructura orgánica básica de este departamento ministerial por el Real Decreto 501/2024, de 21 de mayo, por el que se desarrolla la estructura orgánica básica del Ministerio de Inclusión, Seguridad Social y Migraciones, y se modifica el Real Decreto 1009/2023, de 5 de diciembre, por el que se establece la estructura orgánica básica de los departamentos ministeriales.

Esta Política de Seguridad de la Información (en adelante PSI) es el instrumento en que se apoya el Ministerio de Inclusión, Seguridad Social y Migraciones para alcanzar sus objetivos utilizando de forma segura los sistemas de información y las comunicaciones. La seguridad, concebida como proceso integral, comprende todos los elementos técnicos, humanos, materiales y organizativos relacionados con los sistemas de información y las comunicaciones y debe entenderse no como un producto sino como un proceso continuo de adaptación y mejora, que debe ser controlado, gestionado y monitorizado, implementando la cultura de la seguridad en el Ministerio.

La PSI constituye el marco de referencia orientado a facilitar la definición, gestión, administración e implementación de los mecanismos y procedimientos de seguridad establecidos en el Esquema Nacional de Seguridad. Identifica responsabilidades y establece principios y directrices para una protección adecuada y consistente de los servicios y activos de información gestionados por medio de las Tecnologías de la Información y de las Comunicaciones.

Del mismo modo, el Real Decreto 311/2022, de 3 de mayo, determina que la PSI debe ser coherente con lo establecido en el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales, y la normativa vigente en esta materia, prevaleciendo éstos en lo relativo a la protección de datos de carácter personal en caso de discrepancias.

En este sentido, la entrada en vigor del citado Reglamento Europeo (UE) 2016/679, y de la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales, plantea nuevos retos, así como la necesidad de dar un nuevo enfoque al tratamiento de datos de carácter personal. De este modo, para garantizar su adecuada implantación resulta necesario intensificar la labor de coordinación con el resto de las normas de obligatoria implantación en la organización, especialmente con el Esquema Nacional de Seguridad, buscando sinergias en el desarrollo de ambas. Para garantizar la coordinación en la implantación de estas normativas se deberá procurar que:

a) El cumplimiento del Esquema Nacional de Seguridad y la legislación de protección de datos estén alineados, apoyándose mutuamente en el caso de los sistemas de información que tratan datos de carácter personal.

b) Los planes de concienciación y formación que se definan contengan contenidos comunes en el ámbito de los tratamientos de datos de carácter personal.

c) Se establezca la correspondencia entre los tratamientos de datos de carácter personal y los sistemas de información identificados en el Esquema Nacional de Seguridad que incluyan datos de carácter personal, buscando unificar en una única declaración los requisitos y medidas de seguridad y de protección de los datos personales que son necesarios para cumplir con ambas normas.

d) Las auditorías de cumplimiento en particular y las revisiones de seguridad en general que incluyan controles de ambas normas, se efectúen de manera conjunta.

e) Se lleve a cabo una designación común de las responsabilidades, así como una relación con los organismos reguladores y de coordinación.

La PSI es de obligado cumplimiento para todo el personal que acceda a los sistemas de información o a la información del departamento, para sus órganos superiores y directivos que no tengan establecida su propia política de seguridad y para los aspectos no tratados en dichas políticas de seguridad particulares.

Esta orden se estructura en veinte artículos, tres disposiciones adicionales, dos disposiciones derogatorias y dos disposiciones finales. La disposición derogatoria primera deroga, en lo que afecta a las competencias del Ministerio de Inclusión, Seguridad Social y Migraciones, la Orden TIN/3016/2011, de 28 de octubre, por la que se crea el Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Ministerio de

Trabajo e Inmigración, y la Orden comunicada de la Ministra de Empleo y Seguridad Social, de 30 de julio de 2012, por la que se aprueba la Política de Seguridad de los Sistemas de Información del Ministerio de Empleo y Seguridad Social. También se deroga en la disposición derogatoria segunda la Orden ISM/254/2021, de 16 de marzo, por la que se crea y regula la Comisión Asesora de Estudios y se establece la regulación del Programa anual de Estudios del departamento, por tratarse de otra norma de naturaleza organizativa de acuerdo con las competencias de la Subsecretaría de Inclusión, Seguridad Social y Migraciones previstas en el Real Decreto 501/2024, de 21 de mayo.

La norma se ajusta a los principios de buena regulación contenidos en el artículo 129 de la Ley 39/2015, de 1 de octubre. En concreto, se adecúa a los principios de necesidad y eficacia puesto que, con la aprobación de la norma, se dota al departamento ministerial de un marco que garantiza la seguridad en la utilización de sus activos de información.

Asimismo, es también adecuada al principio de proporcionalidad, en cuanto se trata de una norma puramente organizativa que, en consecuencia, no restringe derechos ni libertades ni impone obligaciones.

Igualmente, a la vista de su objeto y contenido se considera cumplido el principio de eficiencia en la medida en que la norma prevé que los medios personales y financieros a utilizar son los ya existentes en el ministerio y, además, no se imponen cargas administrativas ni se afecta a las existentes.

Finalmente, se ajusta al principio de seguridad jurídica, pues resulta plenamente coherente con el resto del ordenamiento jurídico, y se da cumplimiento al principio de transparencia al quedar claramente delimitados los objetivos y fines perseguidos por esta orden ministerial.

En el proceso de su tramitación se han recabado informes de la Comisión Permanente de la Comisión Ministerial de Administración Digital del Ministerio de Inclusión, Seguridad Social y Migraciones, del delegado de protección de datos y de la Secretaría General Técnica del mismo ministerio, así como de la Agencia Española de Protección de Datos.

En su virtud, con la aprobación previa del Ministro para la Transformación Digital y de la Función Pública, dispongo:

Artículo 1. *Objeto y ámbito de aplicación.*

1. El objeto de esta orden es la aprobación de la Política de Seguridad de la Información (en adelante PSI) en el ámbito del Ministerio de Inclusión, Seguridad Social y Migraciones, su marco organizativo y tecnológico, así como la creación del Comité de Seguridad de los Sistemas de Información y la regulación de su composición, funcionamiento y funciones.

2. La PSI será de obligado cumplimiento para todos los órganos superiores y directivos del Ministerio de Inclusión, Seguridad Social y Migraciones, con las excepciones que, en su caso, correspondan a la Secretaría de Estado de la Seguridad Social y Pensiones y a las entidades gestoras y servicios comunes de la Administración de la Seguridad Social adscritas a la misma.

3. Se podrán adscribir a la presente PSI aquellos organismos y entidades de derecho público vinculados o dependientes del Ministerio de Inclusión, Seguridad Social y Migraciones que no tengan establecida su propia política de seguridad y así lo soliciten.

4. La PSI será de obligado cumplimiento para todo el personal que acceda tanto a los sistemas de información como a la propia información que sea gestionada por el departamento, con independencia de cuál sea su destino, adscripción o relación.

Artículo 2. *Misión del departamento.*

El Ministerio de Inclusión, Seguridad Social y Migraciones es el departamento encargado de la propuesta y ejecución de la política del Gobierno en materia de Seguridad Social y clases pasivas, así como de la elaboración y el desarrollo de la política del Gobierno en materia de extranjería, inmigración y emigración y de políticas de inclusión, de conformidad con lo establecido en el artículo 1 del Real Decreto 501/2024, de 21 de mayo, por el que se desarrolla la estructura orgánica básica del Ministerio de Inclusión, Seguridad Social y Migraciones, y se modifica el Real Decreto 1009/2023, de 5 de diciembre, por el que se establece la estructura orgánica básica de los departamentos ministeriales.

Artículo 3. *Marco normativo.*

El marco normativo en que se desarrollan las actividades del Ministerio de Inclusión, Seguridad Social y Migraciones en el ámbito de la prestación de los servicios electrónicos a la ciudadanía, sin perjuicio de la legislación específica, está integrado fundamentalmente por las siguientes disposiciones:

a) Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

b) Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

c) Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

d) Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

e) Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.

f) Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

g) Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.

h) Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

i) Ley 12/1989, de 9 de mayo, de la Función Estadística Pública.

j) Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.

k) Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

l) Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica.

m) Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

n) Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en al ámbito de la Administración Electrónica.

o) Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

p) Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional.

q) Orden ISM/11/2021, de 12 de enero, por la que se crea y regula la Sede Electrónica Central del Ministerio de Inclusión, Seguridad Social y Migraciones.

r) Orden TIN 1459/2010, de 28 de mayo, por la que se crea la Sede Electrónica de la Secretaría de Estado de la Seguridad Social.

s) Aquellas normas aplicables a la administración electrónica y seguridad de la información derivadas de las anteriores y publicadas en las sedes electrónicas dentro del ámbito de aplicación de la PSI del Ministerio.

Artículo 4. *Principios de la seguridad de la información.*

1. Principios básicos.

Los principios básicos son directrices fundamentales de seguridad que han de tenerse siempre presentes en cualquier actividad relacionada con el uso de los activos de información. Estos principios básicos, en su continuo fortalecimiento y revisión, se ajustarán en todo caso, de acuerdo con lo previsto en la disposición adicional segunda del Real Decreto 311/2022, de 3 de mayo, a las instrucciones técnicas de seguridad que publique la Secretaría de Estado de Función Pública del Ministerio para la Transformación Digital y de la

Función Pública, así como a las guías de seguridad de las tecnologías de la información y la comunicación (guías CCN-STIC) Complementando lo dispuesto en el capítulo II del Real Decreto 311/2022, de 3 de mayo, se establecen los siguientes principios básicos:

a) Alcance estratégico: la seguridad de la información debe contar con el compromiso y apoyo de todos los niveles directivos, de forma que pueda estar coordinada e integrada con el resto de iniciativas estratégicas del departamento para conformar un todo coherente y eficaz.

b) Responsabilidad diferenciada: en los sistemas de información se diferenciará la persona responsable de la información, que determina los requisitos de seguridad de la información tratada; la persona responsable del servicio, que determina los requisitos de seguridad de los servicios prestados; la persona responsable del sistema, que tiene la responsabilidad de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad; y la persona responsable de la seguridad, que será distinta de la responsable del sistema, no debiendo existir dependencia jerárquica entre ambas, y que determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones. En los supuestos de tratamientos de datos personales se identificará además a la persona, organismo o unidad responsable de tratamientos y, en su caso, al encargado de tratamiento, de acuerdo con las definiciones del artículo 4.7 y 8 del Reglamento (UE) 2016/679.

c) Seguridad integral: la seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema de información, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas de información.

d) Gestión de los riesgos: el análisis y gestión de los riesgos será parte esencial del proceso de seguridad. La gestión de los riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción a estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerán un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos, y la eficacia y el coste de las medidas de seguridad. Además, las medidas de seguridad deberán garantizar el cumplimiento de lo previsto en el artículo 32 del Reglamento (UE) 2016/679, por lo que el responsable del tratamiento de datos personales, y en su caso, de los encargados del tratamiento, podrán adoptar todas aquellas medidas adicionales con el fin de garantizar la seguridad de los datos personales, en virtud de lo dispuesto en los artículos 24 y 25 del Reglamento (UE) 2016/679, en el artículo 28 de la Ley Orgánica 3/2018, de 5 de diciembre, y en el artículo 3 del Real Decreto 311/2022, de 3 de mayo.

e) Proporcionalidad: el establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.

f) Mejora continua: las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado, instruido y con dichas competencias entre sus funciones.

g) Seguridad desde el diseño y por defecto: los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto. Además, con el fin de garantizar la resiliencia y la protección de los datos personales, se deben tener en cuenta las medidas de seguridad por defecto en base a los artículos 24 y 25 del Reglamento (UE) 2016/679, así como las medidas de seguridad orientadas al riesgo según el artículo 32 del Reglamento (UE) 2016/679.

h) Vigilancia continua: de forma que la evaluación permanente del estado de la seguridad de los activos permita medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración. En cuanto a la gestión de incidentes que afecten a datos

personales, se tendrán en cuenta las obligaciones específicas de notificación, comunicación y documentación especificadas en los artículos 33 y 34 del Reglamento (UE) 2016/679.

2. Principios particulares y responsabilidades específicas.

Las directrices fundamentales de seguridad se concretan en un conjunto de principios particulares y responsabilidades específicas, que se configuran como objetivos instrumentales que garantizan el cumplimiento de los principios básicos de la PSI y que inspiran las actuaciones del departamento en dicha materia. Se establecen los siguientes principios particulares y responsabilidades específicas:

a) Protección de datos de carácter personal: se adoptarán las medidas técnicas y organizativas destinadas a garantizar el nivel de seguridad exigido por la normativa vigente en relación con el tratamiento de los datos de carácter personal.

b) Gestión de activos de información: los activos de información del departamento se encontrarán inventariados y categorizados, y estarán asociados a un responsable.

c) Seguridad ligada a las personas: se implantarán los mecanismos necesarios para que cualquier persona que acceda o pueda acceder a los activos de información, conozca sus responsabilidades, y, de este modo, se reduzca el riesgo derivado de un uso indebido de dichos activos.

d) Seguridad física: los activos de información serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.

e) Seguridad en la gestión de comunicaciones y operaciones: se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las Tecnologías de la Información y Comunicaciones. La información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad. Para proteger las redes del departamento, se analizará el tráfico cifrado de usuarios de forma automatizada. Se realizará la excepción en este análisis de las categorías de navegación relacionadas con datos sensibles especialmente protegidos de acuerdo con la normativa de protección de datos vigente, siempre que sea posible la discriminación.

f) Control de acceso: se limitará el acceso a los activos de información por parte de usuarios, procesos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo. Además, quedará registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso y auditar su uso adecuado, conforme a la actividad de la organización.

g) Adquisición, desarrollo y mantenimiento de los sistemas de información: se contemplarán los aspectos de seguridad de la información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.

h) Gestión de los incidentes de seguridad: se implantarán los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.

i) Gestión de la continuidad: se implantarán los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de sus procesos de negocio, de acuerdo con las necesidades de nivel de servicio de sus usuarios.

j) Cumplimiento: se adoptarán las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información.

3. Sin perjuicio de lo establecido en los apartados 1 y 2, la presente PSI se establecerá en base a los principios básicos y se desarrollará aplicando los requisitos mínimos contemplados en el capítulo II y en el artículo 12.6 del Real Decreto 311/2022, de 3 de mayo.

4. Estos principios particulares, en su continuo fortalecimiento y revisión, se ajustarán en todo caso a las instrucciones técnicas de seguridad que publique la Secretaría de Estado de Función Pública del Ministerio para la Transformación Digital y de la Función Pública, así como a las guías CCN-STIC.

Artículo 5. *Estructura organizativa.*

La gestión de la seguridad en el Ministerio de Inclusión, Seguridad Social y Migraciones se apoya en la siguiente estructura organizativa:

a) La persona responsable del sistema global de información.
b) El Comité de Seguridad de los Sistemas de Información.
c) La persona responsable de sistemas de información.
d) La persona responsable de seguridad del Ministerio de Inclusión, Seguridad Social y Migraciones.
e) La persona responsable de la prestación del servicio.
f) El delegado o la delegada de protección de datos.

Artículo 6. *Persona responsable del sistema global de información.*

1. La persona titular de la Subsecretaría de Inclusión, Seguridad Social y Migraciones es la responsable del sistema global de información, y, además, es la responsable última del funcionamiento de los servicios.

El sistema global de información integra todos los sistemas de información de los órganos superiores y directivos y unidades dependientes del Ministerio de Inclusión, Seguridad Social y Migraciones, de los que son responsables las personas titulares de estos.

2. La persona responsable del sistema global de información tiene las siguientes funciones:

a) Hacer cumplir las disposiciones establecidas en el Esquema Nacional de Seguridad y en la Ley Orgánica 3/2018, de 5 de diciembre, cuando el sistema de información se encuentre dentro del ámbito de aplicación de estas y, en su caso, emitir directrices.

b) Resolver los conflictos que puedan surgir entre los distintos responsables de los sistemas de información, en el ejercicio de sus funciones, en los términos establecidos en el artículo 18.

Artículo 7. *Comité de Seguridad de los Sistemas de Información.*

1. Se crea el Comité de Seguridad de los Sistemas de Información (en adelante CSSI) que coordinará todas las actividades relacionadas con la seguridad de los sistemas de información en el ámbito del Ministerio de Inclusión, Seguridad Social y Migraciones. En los casos en los que el CSSI así lo decida, éste podrá asumir las funciones de responsable del sistema de información y de responsable de la prestación del servicio.

2. Como órgano colegiado de carácter transversal adscrito a la Subsecretaría de Inclusión, Seguridad Social y Migraciones, el CSSI tendrá la siguiente composición:

a) Presidencia: la persona titular de la Subsecretaría de Inclusión, Seguridad Social y Migraciones.

b) Vicepresidencia: la persona titular del Gabinete Técnico de la Subsecretaría.

c) Vocalías:

i) Una vocalía en representación de cada uno de los órganos superiores y directivos del Ministerio de Inclusión, Seguridad Social y Migraciones, con rango igual o superior a Dirección General o equivalente. La persona designada deberá tener un rango mínimo de subdirector general o asimilado.

ii) Una vocalía para la persona responsable de seguridad del Ministerio de Inclusión, Seguridad Social y Migraciones.

iii) Una vocalía para la persona titular de la Subdirección General de Tecnologías de la Información y Comunicaciones del Ministerio de Inclusión, Seguridad Social y Migraciones que, además, actuará como secretaria del CSSI.

iv) Una vocalía para la persona titular de la Gerencia de Informática de la Seguridad Social.

v) Una vocalía para el delegado o la delegada de protección de datos del Ministerio de Inclusión, Seguridad Social y Migraciones, que actuará como asesor con voz, pero sin voto, para garantizar su independencia en atención a la naturaleza de sus funciones de asistencia y apoyo.

3. En caso de vacante, ausencia o enfermedad, así como en los casos en que haya sido declarada su abstención o recusación y, en general, cuando concurra alguna causa justificada, se establece el siguiente régimen de suplencias de los miembros del CSSI:

a) La presidencia será sustituida por la vicepresidencia.
b) Las vocalías serán sustituidas por sus suplentes, que deberán ser personal funcionario pertenecientes al grupo A1, con nivel 28 o superior.

4. El CSSI tiene las siguientes funciones:

a) Definir y aprobar los planes estratégicos, líneas de actuación y objetivos en materia de seguridad del Ministerio de Inclusión, Seguridad Social y Migraciones, siempre alineados con la misión y objetivos de la organización.
b) Garantizar la divulgación de la PSI.
c) La aprobación y seguimiento de las normas y procedimientos en materia de seguridad que afecten transversalmente al Ministerio de Inclusión, Seguridad Social y Migraciones.
d) Establecer, cuando sea posible, criterios comunes de actuación en todos los órganos superiores y directivos de la organización para el cumplimiento de las normas o procedimientos en materia de seguridad de la información que sean de aplicación.
e) Revisar el estado global de la seguridad en cada uno de los órganos superiores y directivos dependientes del Ministerio de Inclusión, Seguridad Social y Migraciones.
f) Trasladar las directrices que sean establecidas por el CSSI a cada uno de los órganos superiores y directivos y garantizar su cumplimiento.
g) Actualizar y asignar las funciones y obligaciones de la PSI de cada uno de los responsables definidos en el artículo 2.
h) Promover líneas de trabajo para una adecuada concienciación y formación en materia de seguridad para el personal del Ministerio de Inclusión, Seguridad Social y Migraciones.
i) Ser informado, deliberar e intercambiar información con los órganos superiores y directivos del Ministerio de Inclusión, Seguridad Social y Migraciones que sean responsables de tratamientos con datos de carácter personal para tratar y asesorar sobre las medidas de seguridad técnica y las medidas de protección de la información aplicables en los sistemas y servicios que les afecten.

5. El CSSI se reunirá con carácter ordinario como mínimo tres veces al año y, con carácter extraordinario, cuando la presidencia lo considere necesario. Las sesiones se celebrarán de forma presencial o a distancia, lo que se especificará necesariamente en la convocatoria.
6. El CSSI podrá recabar del personal técnico, propio o externo, la información pertinente para la toma de sus decisiones. Asistirán en su caso en calidad de asesores con voz, pero sin voto.
7. La secretaría del CSSI levantará el acta de cada reunión del comité y realizará, junto con la persona responsable de seguridad del departamento, todos los trabajos previos necesarios apoyándose cuando lo requiera en las unidades y organismos del departamento.
8. En lo no previsto en esta orden, el funcionamiento del CSSI se ajustará a lo dispuesto en materia de órganos colegiados por la sección 3.ª del capítulo II del título preliminar de la Ley 40/2015, de 1 de octubre.

Artículo 8. *Persona responsable de sistemas de información.*

1. Las personas responsables de los sistemas de información garantizan, en sus respectivos ámbitos, la puesta en marcha, mantenimiento y actualización de las medidas pertinentes en materia de seguridad de los sistemas de información. Asimismo, determinan los requisitos de seguridad de la información tratada, de los tratamientos realizados sobre la misma y de los servicios electrónicos que se prestan, en sus respectivos ámbitos.
2. Se designan como responsables de sus sistemas de información a las personas titulares de todos los órganos superiores y directivos del Ministerio de Inclusión, Seguridad Social y Migraciones y a las personas titulares de todos los organismos adscritos y órganos dependientes de los órganos superiores y directivos del Ministerio de Inclusión, Seguridad Social y Migraciones para la información que tratan en el ejercicio de sus competencias, sin

perjuicio de que estos puedan delegar ciertas funciones en las direcciones y subdirecciones provinciales correspondientes.

3. Las personas responsables de los sistemas de información son responsables del tratamiento, responsables de la información y responsables de los servicios electrónicos en todos los sistemas de información que traten datos personales.

4. A las personas responsables de los sistemas de información les corresponden las siguientes funciones:

a) Garantizar que se gestiona el riesgo de seguridad de sus sistemas de información.

b) Definir los requisitos de seguridad de los sistemas de información de los que son responsables y, para cada uno de ellos, su nivel de riesgo residual aceptable.

c) Suspender el manejo de una determinada información o la prestación de un servicio si es informado de deficiencias graves de seguridad.

d) Adoptar las medidas necesarias para que el personal con acceso a sus sistemas de información conozca las normas de seguridad que debe aplicar.

e) Identificar y valorar la criticidad de la información que manejan y determinar en función de esta los requisitos de seguridad que es necesario cumplir para cada tipo de información.

f) Determinar el ciclo de vida de la información manejada y determinar los procedimientos de creación, tratamiento y destrucción de esta.

g) En cuanto a tratamientos con datos personales, deberán satisfacer los derechos de las personas titulares de los datos, registrar la condición que legitima el tratamiento, atender los derechos de información, acceso, rectificación, oposición, supresión («derecho al olvido»), limitación del tratamiento, portabilidad y de no ser objeto de decisiones individuales automatizadas y realizar la evaluación de impacto en la privacidad.

h) Comunicar al delegado o delegada de protección de datos correspondiente, con carácter previo a su uso, los nuevos tratamientos de alto riesgo con datos personales.

Artículo 9. *Persona responsable de la prestación del servicio.*

1. La persona responsable de la prestación del servicio tiene la obligación de implementar las medidas de seguridad sugeridas por la persona responsable de seguridad, que están incluidas en el plan director de seguridad.

2. Se designa como persona responsable de la prestación del servicio a la persona titular de la Subdirección General de Tecnologías de la Información y Comunicaciones, sin perjuicio de que pueda delegar ciertas funciones.

3. La persona responsable de la prestación del servicio tiene las siguientes funciones:

a) Implementar las medidas de seguridad que entren en su ámbito de actuación establecidas en el plan director de seguridad elaborado por la persona responsable de seguridad y aprobado por la persona responsable del sistema de información.

b) Observar el cumplimiento de las normas y procedimientos establecidos y aprobados por el CSSI en la administración y operativa habitual de los sistemas de información.

c) Supervisar y garantizar la gestión, configuración y actualización de los recursos que soportan el funcionamiento correcto de los sistemas de información y de la prestación de los servicios.

d) Colaborar en las auditorias llevadas a cabo por la persona responsable de seguridad, y aportar información completa y veraz sobre el estado de las medidas de seguridad implantadas que sean de su responsabilidad.

Artículo 10. *Persona responsable de seguridad.*

1. La persona responsable de seguridad es la encargada de determinar las decisiones para satisfacer los requisitos de seguridad de la información, los tratamientos y los servicios electrónicos.

2. La Subdirección General de Tecnologías de la Información y Comunicaciones designará a la persona responsable de seguridad preservando la debida independencia y sin perjuicio de que ésta pueda delegar ciertas funciones. Las personas titulares de todos los órganos superiores y directivos del Ministerio de Inclusión, Seguridad Social y Migraciones podrán nombrar su propio responsable de seguridad en su ámbito de competencia.

3. La persona responsable de seguridad tiene las siguientes funciones:

a) Determinar las decisiones necesarias para satisfacer los requisitos de seguridad de la información, de los tratamientos y de los servicios que hayan sido establecidos por sus respectivos responsables.

b) Realizar periódicamente un proceso de análisis de los riesgos de los sistemas de información que permita identificar los riesgos a los que éste se encuentra expuesto y las medidas para asegurar el nivel de riesgo residual aceptable aprobado para cada sistema de información.

c) Establecer el conjunto de proyectos y actuaciones que conformarán el plan director de seguridad que permitirá implantar las medidas de seguridad propuestas, y elevarlo al responsable global del sistema de información.

d) Realizar el seguimiento y control del estado de la seguridad del sistema de información y verificar que las medidas de seguridad definidas son adecuadas para la protección de la información y los servicios.

e) Realizar las auditorias periódicas que se determinen en cada sistema de información, incluyendo las revisiones relativas a protección de datos, para garantizar la correcta aplicación de las medidas de seguridad y el cumplimiento de las normas y procedimientos vigentes en la organización. El informe resultante de las mismas se enviará a las personas responsables de los sistemas de información y a las personas responsables de la prestación del servicio para subsanar las deficiencias encontradas.

f) Redactar, cuando sea necesario, las declaraciones de aplicabilidad de los sistemas de información respecto al Esquema Nacional de Seguridad.

g) Asistir al delegado o delegada de protección de datos del Ministerio de Inclusión, Seguridad Social y Migraciones y, en su caso, al delegado o delegada de protección de datos de la Secretaría de Estado de la Seguridad Social y Pensiones, en cuantas actuaciones relativas a la seguridad de los sistemas de información en las que sean requeridos.

h) Aprobar planes de formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad y elevarlos al CSSI para su incorporación en los planes de los organismos o unidades dependientes del Ministerio de Inclusión, Seguridad Social y Migraciones, así como establecer actuaciones disuasorias a favor de la seguridad.

Artículo 11. *Delegado o delegada de protección de datos.*

1. El delegado o la delegada de protección de datos, designado en virtud de lo dispuesto en el artículo 10.3.j) del Real Decreto 501/2024, de 21 de mayo, por el que se desarrolla la estructura orgánica básica del Ministerio de Inclusión, Seguridad Social y Migraciones, y se modifica el Real Decreto 1009/2023, de 5 de diciembre, por el que se establece la estructura orgánica básica de los departamentos ministeriales, en virtud de lo establecido en el Reglamento (UE) 2016/679 y en la Ley Orgánica 3/2018, de 5 de diciembre, es único para todo el departamento, sin perjuicio de la existencia del delegado o delegada de protección de datos de la Secretaría de Estado de la Seguridad Social y Pensiones.

2. En el ámbito de los tratamientos de datos personales, y sin perjuicio de las atribuciones establecidas en el Reglamento (UE) 2016/679 de forma exclusiva a los responsables y encargados de los tratamientos de datos personales, y de las atribuciones exclusivas de las personas responsables de la seguridad, el delegado o delegada de protección de datos ejercerá labores de asesoramiento y supervisión en el ámbito de la presente norma.

3. El delegado o delegada de protección de datos prestará asistencia y asesoramiento a las personas responsables del tratamiento a la hora de identificar los riesgos y adoptar medidas para la protección de los datos personales, y en cuanto a la supervisión de que las mismas se han adoptado y llevado a la práctica. En cualquier caso, las funciones ejecutivas de toma de las decisiones oportunas al respecto serán responsabilidad de los respectivos responsables del tratamiento.

4. El delegado o delegada de protección de datos ejercerá labores de asistencia y asesoramiento a las personas responsables del tratamiento de datos personales, a las personas responsables de la seguridad y a las personas responsables del sistema, en los

procesos de gestión de brechas de datos personales en el ámbito de la gestión general de incidentes de seguridad.

5. El delegado o delegada de protección de datos prestará asesoramiento a las personas responsables de la seguridad y a las personas responsables del sistema, en cuanto a la implantación de medidas de seguridad que tengan un objeto distinto que la protección de datos, en la medida en que impliquen un tratamiento adicional de datos personales, tal y como dispone el artículo 24 del Real Decreto 311/2022, de 3 de mayo.

6. El delegado o delegada de protección de datos participará en el CSSI en materia de protección de datos personales en el compartido objetivo de procurar:

a) Alinear las respectivas normativas de cumplimiento, así como la definición e implantación de medidas de seguridad.

b) Impulsar y/o coordinar auditorías y revisiones del estado de cumplimiento de los requisitos y principios de la legislación aplicable.

c) Diseñar planes de formación y concienciación conjuntos con los de seguridad de la información.

Artículo 12. *Los responsables y los encargados de tratamiento de datos personales.*

1. El responsable de tratamiento es la persona física o jurídica, autoridad pública, servicio u otra entidad que, solo o junto con otros, determina los fines y medios del tratamiento y aplica las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con la normativa vigente en materia de protección de datos personales.

La identidad del responsable de tratamiento figura en el registro de las actividades de tratamiento efectuadas bajo su responsabilidad, de acuerdo con lo dispuesto en el artículo 30 del Reglamento (UE) 2016/679.

2. El encargado de tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que trata datos personales por cuenta del responsable del tratamiento.

Artículo 13. *Gestión de los riesgos.*

1. Se realizará de forma periódica un proceso de análisis de riesgos sobre los sistemas de información, conforme a los principios de gestión de la seguridad basada en los riesgos y reevaluación periódica establecidos en el Esquema Nacional de Seguridad.

2. La persona responsable de seguridad es la encargada de realizar el análisis de riesgos de los sistemas de información, garantizando que el mismo se lleva a cabo de forma correcta y completa, y comunicando los resultados a las personas responsables de los sistemas de información. Además, realizará el seguimiento y control de las acciones a realizar como consecuencia de los resultados del análisis de riesgos.

3. La persona responsable del sistema de información es quien gestiona y asume los riesgos sobre sus sistemas de información.

Artículo 14. *Estructura de la documentación de seguridad del Ministerio de Inclusión, Seguridad Social y Migraciones.*

1. La presente PSI debe ser desarrollada en diferente documentación de seguridad que detalle y concrete los requisitos de seguridad de la información y los servicios, las tareas necesarias para garantizar su cumplimiento y las responsabilidades de todo el personal implicado en las mismas.

2. En el Ministerio de Inclusión, Seguridad Social y Migraciones esta documentación de seguridad se estructura en los siguientes niveles:

a) La PSI: documento con el conjunto de directrices que rigen la forma en que el Ministerio de Inclusión, Seguridad Social y Migraciones gestiona y protege la información que trata y los servicios que presta.

b) Las normas de seguridad: conjunto de documentos que determinan los objetivos de seguridad y directrices generales en cada ámbito concreto y que establecen las responsabilidades del personal implicado. Deben ser globales, concisas y definir puntos de

contacto para su interpretación correcta. Serán aprobadas por el CSSI y serán de obligado cumplimiento en toda la organización.

c) Los procedimientos de seguridad: conjunto de documentos que describen explícitamente y paso a paso cómo realizar determinadas tareas para cumplir lo estipulado en las normas de seguridad. Cada procedimiento debe detallar al menos en qué condiciones debe aplicarse, quienes deben llevarla a cabo y qué hacer en cada momento. Serán de obligado cumplimiento en su ámbito correspondiente, pero no requieren aprobación del CSSI.

d) Las guías de seguridad: documentación que incluye recomendaciones de actuación para mejorar la eficacia y eficiencia de los procedimientos de seguridad, suministra información adicional de apoyo y propone buenas prácticas. No se consideran de obligado cumplimiento ni requieren aprobación del CSSI, proporcionándose a título meramente informativo.

Artículo 15. *Protección de datos de carácter personal.*

1. Se aplicarán a los datos de carácter personal que sean objeto de tratamiento por parte del Ministerio de Inclusión, Seguridad Social y Migraciones, las medidas técnicas y organizativas, y de seguridad apropiadas derivadas del análisis de riesgos, así como de la evaluación de impacto relativa a la protección de datos, que se detalla en el Reglamento (UE) 2016/679 y en la Ley Orgánica 3/2018, de 5 de diciembre.

Además, se aplicarán las medidas correspondientes al anexo II del Real Decreto 311/2022, de 3 de mayo. En el caso de que el análisis de riesgos determine medidas agravadas respecto a la normativa recogida en las medidas del citado anexo, las medidas derivadas del análisis de riesgos serán las que se implementarán en la protección de datos de carácter personal.

En particular, se tendrá en cuenta el artículo 32 del Reglamento (UE) 2016/679, en cuanto a la exigencia de una identificación de riesgos específicos para los derechos y libertades de las personas en relación a los tratamientos de datos personales, que debe ser previo al análisis de riesgos de los sistemas donde se implementen dichos tratamientos, de forma que el nivel de seguridad sea adecuado al riesgo que los tratamientos de datos personales suponen para los derechos y libertades de las personas.

2. Los servicios de ciberseguridad y administración de sistemas, dependientes de los respectivos responsables de los sistemas, podrán implementar tratamientos de datos personales como consecuencia de la implantación de medidas de seguridad que tengan un objeto distinto que la protección de los datos personales, en base a lo dispuesto en el artículo 24 del Real Decreto 311/2022, de 3 de mayo, y teniendo en cuenta, entre otros, los principios de limitación de finalidad; prohibición del tratamiento de los datos personales para fines distintos; el principio de minimización de datos, identificando los datos personales o las categorías de datos personales que pudieran ser tratados; o del principio de limitación del plazo de conservación, identificando los plazos máximos de conservación de los datos personales.

Artículo 16. *Responsabilidad del personal.*

Todo el personal que forme parte del Ministerio de Inclusión, Seguridad Social y Migraciones o que colabore con él en el ejercicio de sus funciones, deberá conocer y aplicar en su ámbito de actuación esta PSI, así como las normas y procedimientos de seguridad de cada sistema de información al que tenga acceso. Estas normas y procedimientos les serán proporcionadas por la persona responsable de cada sistema de información.

Artículo 17. *Relación con otras administraciones públicas.*

Cuando el Ministerio de Inclusión, Seguridad Social y Migraciones preste servicios o ceda información a otras administraciones públicas, les hará partícipes de esta PSI y de las normas de seguridad que apliquen. Las administraciones públicas receptoras quedarán sujetas a las obligaciones establecidas en ellas, debiendo desarrollar sus propios procedimientos para satisfacerlas.

Artículo 18. *Resolución de conflictos.*

En caso de conflicto entre los diferentes responsables, éste será resuelto por el superior jerárquico de los mismos. En defecto de lo anterior, prevalecerá la decisión de la persona responsable del sistema global de información.

Artículo 19. *Formación y concienciación.*

1. El CSSI, en coordinación con la Subdirección General de Recursos Humanos e Inspección de Servicios del Ministerio de Inclusión, Seguridad Social y Migraciones, desarrollará actividades específicas orientadas a la formación y concienciación de su personal en materia de seguridad de la información, así como a la difusión de la presente PSI y su desarrollo normativo, en particular entre el personal de nueva incorporación. A estos efectos, los planes de formación del Ministerio de Inclusión, Seguridad Social y Migraciones incluirán actividades formativas específicas sobre esta materia.

2. El CSSI promoverá una cultura de seguridad de la información alineada con la PSI entre aquellas organizaciones y usuarios externos que tengan acceso por acuerdo o convenio a sus sistemas de información.

Artículo 20. *Actualización y revisión periódica.*

1. La PSI deberá mantenerse actualizada para adecuarla al progreso de los servicios de la administración electrónica, a la evolución tecnológica y al desarrollo de la sociedad de la información, así como a los estándares internacionales de seguridad.

2. Las propuestas de revisión de la PSI se elaborarán por el CSSI que, con tal objetivo, revisará regularmente la oportunidad, idoneidad, completitud y precisión de lo establecido en la misma.

Disposición adicional primera. *No incremento del gasto público.*

Las medidas incluidas en esta orden no supondrán incremento del gasto, siendo atendidas con los medios personales, técnicos y presupuestarios asignados al Ministerio de Inclusión, Seguridad Social y Migraciones.

Disposición adicional segunda. *Deber de colaboración en la implantación de la PSI.*

Todos los órganos superiores y directivos del Ministerio de Inclusión, Seguridad Social y Migraciones y sus organismos adscritos y órganos dependientes colaborarán en las actuaciones de implementación de la PSI aprobada por esta orden.

Disposición adicional tercera. *Vigencia de políticas y normas de seguridad.*

Todas las políticas y normas de seguridad anteriores a la publicación de esta PSI permanecerán vigentes mientras no se acuerde por el CSSI la publicación de una nueva que la sustituya.

Cualquier actuación posterior a la publicación de esta PSI relativo a políticas o normas de seguridad deberán ser informados al CSSI con el objetivo de mantener unas líneas estratégicas de gestión de la seguridad de la información y de la protección de datos personales coherentes y complementarias.

Disposición derogatoria primera. *Derogación normativa.*

Quedan derogadas las disposiciones de igual o inferior rango en lo que se opongan a lo dispuesto en esta orden ministerial, y en particular, en lo que afecta a las competencias del Ministerio de Inclusión, Seguridad Social y Migraciones, las siguientes:

a) Orden TIN/3016/2011, de 28 de octubre, por la que se crea el Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Ministerio de Trabajo e Inmigración.

b) Orden comunicada de la Ministra de Empleo y Seguridad Social, de 30 de julio de 2012, por la que se aprueba la Política de Seguridad de los Sistemas de Información del Ministerio de Empleo y Seguridad Social.

Disposición derogatoria segunda. *Derogación normativa.*

Queda derogada la Orden ISM/254/2021, de 16 de marzo, por la que se crea y regula la Comisión Asesora de Estudios y se establece la regulación del Programa anual de Estudios del departamento.

Disposición final primera. *Instrucciones de aplicación.*

La persona titular de la Subsecretaría de Inclusión, Seguridad Social y Migraciones podrá dictar las instrucciones necesarias para el adecuado cumplimiento de esta orden.

Disposición final segunda. *Publicidad de la PSI y entrada en vigor.*

1. La presente orden entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».
2. Esta orden se publicará en la sede electrónica del Ministerio de Inclusión, Seguridad Social y Migraciones y en todas aquellas sedes electrónicas en cuyo ámbito sea de aplicación.

§ 22

Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas

Jefatura del Estado
«BOE» núm. 102, de 29 de abril de 2011
Última modificación: 29 de julio de 2022
Referencia: BOE-A-2011-7630

JUAN CARLOS I

REY DE ESPAÑA

A todos los que la presente vieren y entendieren,

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley.

PREÁMBULO

Los Estados modernos se enfrentan actualmente a diferentes desafíos que confieren a la seguridad nacional un carácter cada vez más complejo. Estos nuevos riesgos, generados, en gran medida, por la globalización, y entre los que se cuentan el terrorismo internacional, la proliferación de armas de destrucción masiva o el crimen organizado, se suman a los ya existentes, de los cuales el terrorismo tradicional venía siendo un exponente.

En este marco, es cada vez mayor la dependencia que las sociedades tienen del complejo sistema de infraestructuras que dan soporte y posibilitan el normal desenvolvimiento de los sectores productivos, de gestión y de la vida ciudadana en general. Estas infraestructuras suelen ser sumamente interdependientes entre sí, razón por la cual los problemas de seguridad que pueden desencadenarse en cascada a través del propio sistema tienen la posibilidad de ocasionar fallos inesperados y cada vez más graves en los servicios básicos para la población.

Hasta tal punto es así, que cualquier interrupción no deseada –incluso de corta duración y debida bien a causas naturales o técnicas, bien a ataques deliberados– podría tener graves consecuencias en los flujos de suministros vitales o en el funcionamiento de los servicios esenciales, además de provocar perturbaciones y disfunciones graves en materia de seguridad, lo que es objeto de especial atención para el Sistema Nacional de Gestión de Situaciones de Crisis.

Dentro de las prioridades estratégicas de la seguridad nacional se encuentran las infraestructuras, que están expuestas a una serie de amenazas. Para su protección se hace imprescindible, por un lado, catalogar el conjunto de aquéllas que prestan servicios esenciales a nuestra sociedad y, por otro, diseñar un planeamiento que contenga medidas de prevención y protección eficaces contra las posibles amenazas hacia tales

infraestructuras, tanto en el plano de la seguridad física como en el de la seguridad de las tecnologías de la información y las comunicaciones.

En esa línea, se han emprendido diversas actuaciones a nivel nacional, como la aprobación, por la Secretaría de Estado de Seguridad del Ministerio del Interior, de un primer Plan Nacional de Protección de las Infraestructuras Críticas, de 7 de mayo de 2007, así como la elaboración de un primer Catálogo Nacional de Infraestructuras Estratégicas. Así mismo, con fecha 2 de noviembre de 2007, el Consejo de Ministros aprobó un Acuerdo sobre Protección de Infraestructuras Críticas, mediante el cual se dio un impulso decisivo en dicha materia. El desarrollo y aplicación de este Acuerdo supone un avance cualitativo de primer orden para garantizar la seguridad de los ciudadanos y el correcto funcionamiento de los servicios esenciales.

Paralelamente, existen también una serie de actuaciones desarrolladas a nivel internacional en el ámbito europeo: tras los terribles atentados de Madrid, el Consejo Europeo de junio de 2004 instó a la Comisión Europea a elaborar una estrategia global sobre protección de infraestructuras críticas. El 20 de octubre de 2004 la Comisión adoptó una Comunicación sobre protección de las infraestructuras críticas en la lucha contra el terrorismo, que contiene propuestas para mejorar la prevención, preparación y respuesta de Europa frente a atentados terroristas que les afecten. Con posterioridad, en diciembre de 2004, el Consejo aprobó el PEPIC (Programa europeo de protección de infraestructuras críticas) y puso en marcha una red de información sobre alertas en infraestructuras críticas (Critical Infrastructures Warning Information Network-CIWIN).

En la actualidad, la entrada en vigor de la Directiva 2008/114, del Consejo, de 8 de diciembre, sobre la identificación y designación de Infraestructuras Críticas Europeas y la evaluación de la necesidad de mejorar su protección (en adelante, Directiva 2008/114/CE), constituye un importante paso en la cooperación en esta materia en el seno de la Unión. En dicha Directiva se establece que la responsabilidad principal y última de proteger las infraestructuras críticas europeas corresponde a los Estados miembros y a los operadores de las mismas, y se determina el desarrollo de una serie de obligaciones y de actuaciones por dichos Estados, que deben incorporarse a las legislaciones nacionales.

Las actuaciones necesarias para optimizar la seguridad de las infraestructuras se enmarcan principalmente en el ámbito de la protección contra agresiones deliberadas y, muy especialmente, contra ataques terroristas, resultando por ello lideradas por el Ministerio del Interior.

Sin embargo, la seguridad de las infraestructuras críticas exige contemplar actuaciones que vayan más allá de la mera protección material contra posibles agresiones o ataques, razón por la cual resulta inevitable implicar a otros órganos de la Administración General del Estado, de las demás Administraciones Públicas, de otros organismos públicos y del sector privado. Estas infraestructuras críticas dependen cada vez más de las tecnologías de la información, tanto para su gestión como para su vinculación con otros sistemas, para lo cual se basan, principalmente, en medios de información y de comunicación de carácter público y abierto. Es preciso contar, por tanto, con la cooperación de todos los actores involucrados en la regulación, planificación y operación de las diferentes infraestructuras que proporcionan los servicios esenciales para la sociedad, sin perjuicio de la coordinación que ejercerá el Ministerio del Interior en colaboración con las Comunidades Autónomas.

En consecuencia, y dada la complejidad de la materia, su incidencia sobre la seguridad de las personas y sobre el funcionamiento de las estructuras básicas nacionales e internacionales, y en cumplimiento de lo estipulado por la Directiva 2008/114/CE, se hace preciso elaborar una norma cuyo objeto es, por un lado, regular la protección de las infraestructuras críticas contra ataques deliberados de todo tipo (tanto de carácter físico como cibernético) y, por otro lado, la definición de un sistema organizativo de protección de dichas infraestructuras que aglutine a las Administraciones Públicas y entidades privadas afectadas. Como pieza básica de este sistema, la Ley crea el Centro Nacional para la Protección de las Infraestructuras Críticas como órgano de asistencia al Secretario de Estado de Seguridad en la ejecución de las funciones que se le encomiendan a éste como órgano responsable del sistema.

La finalidad de esta norma es, por lo tanto, el establecimiento de medidas de protección de las infraestructuras críticas que proporcionen una base adecuada sobre la que se asiente

una eficaz coordinación de las Administraciones Públicas y de las entidades y organismos gestores o propietarios de infraestructuras que presten servicios esenciales para la sociedad, con el fin de lograr una mejor seguridad para aquéllas.

Sobre esta base, se sustentarán el Catálogo Nacional de Infraestructuras Estratégicas (conforme a la comunicación del Consejo de la Unión Europea de 20 de octubre de 2004, que señala que cada sector y cada Estado miembro deberá identificar las infraestructuras que son críticas en sus respectivos territorios) y el Plan Nacional de Protección de Infraestructuras Críticas, como principales herramientas en la gestión de la seguridad de nuestras infraestructuras.

La Ley consta de 18 artículos, estructurados en 3 Títulos. El Título I se destina a las definiciones de los términos acuñados por la Directiva 2008/114/CE, así como a establecer las cuestiones relativas al ámbito de aplicación y objeto. El Título II se dedica a regular los órganos e instrumentos de planificación que se integran en el Sistema de Protección de las Infraestructuras Críticas. El Título III establece, finalmente, las medidas de protección y los procedimientos que deben derivar de la aplicación de dicha norma. Asimismo, la Ley consta de cuatro Disposiciones Adicionales y cinco Disposiciones Finales.

Si bien el contenido material de la Ley es eminentemente organizativo, especialmente en lo concerniente a la composición, competencias y funcionamiento de los órganos que integran el Sistema de Protección de Infraestructuras Críticas, así como en todo lo relativo a los diferentes planes de protección, se ha optado por dotar a esta norma de rango legal, de acuerdo con el criterio del Consejo de Estado, a fin de poder cubrir suficientemente aquellas obligaciones que la Ley impone y que requieren de una cobertura legal específica.

TÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

1. Esta Ley tiene por objeto establecer las estrategias y las estructuras adecuadas que permitan dirigir y coordinar las actuaciones de los distintos órganos de las Administraciones Públicas en materia de protección de infraestructuras críticas, previa identificación y designación de las mismas, para mejorar la prevención, preparación y respuesta de nuestro Estado frente a atentados terroristas u otras amenazas que afecten a infraestructuras críticas. Para ello se impulsará, además, la colaboración e implicación de los organismos gestores y propietarios de dichas infraestructuras, a fin de optimizar el grado de protección de éstas contra ataques deliberados de todo tipo, con el fin de contribuir a la protección de la población.

2. Asimismo, la presente Ley regula las especiales obligaciones que deben asumir tanto las Administraciones Públicas como los operadores de aquellas infraestructuras que se determinen como infraestructuras críticas, según lo dispuesto en los párrafos e) y f) del artículo 2 de la misma.

Artículo 2. *Definiciones.*

A los efectos de la presente Ley, se entenderá por:

a) Servicio esencial: el servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas.

b) Sector estratégico: cada una de las áreas diferenciadas dentro de la actividad laboral, económica y productiva, que proporciona un servicio esencial o que garantiza el ejercicio de la autoridad del Estado o de la seguridad del país. Su categorización viene determinada en el anexo de esta norma.

c) Subsector estratégico: cada uno de los ámbitos en los que se dividen los distintos sectores estratégicos, conforme a la distribución que contenga, a propuesta de los Ministerios y organismos afectados, el documento técnico que se apruebe por el Centro Nacional de Protección de las Infraestructuras Críticas.

d) Infraestructuras estratégicas: las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales.

e) Infraestructuras críticas: las infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.

f) Infraestructuras críticas europeas: aquellas infraestructuras críticas situadas en algún Estado miembro de la Unión Europea, cuya perturbación o destrucción afectaría gravemente al menos a dos Estados miembros, todo ello con arreglo a la Directiva 2008/114, del Consejo, de 8 de diciembre, sobre la identificación y designación de Infraestructuras Críticas Europeas y la evaluación de la necesidad de mejorar su protección (en adelante, Directiva 2008/114/CE).

g) Zona crítica: aquella zona geográfica continua donde estén establecidas varias infraestructuras críticas a cargo de operadores diferentes e interdependientes, que sea declarada como tal por la Autoridad competente. La declaración de una zona crítica tendrá por objeto facilitar la mejor protección y una mayor coordinación entre los diferentes operadores titulares de infraestructuras críticas o infraestructuras críticas europeas radicadas en un sector geográfico reducido, así como con las Fuerzas y Cuerpos de Seguridad del Estado y las Policías Autonómicas de carácter integral.

h) Criterios horizontales de criticidad: los parámetros en función de los cuales se determina la criticidad, la gravedad y las consecuencias de la perturbación o destrucción de una infraestructura crítica se evaluarán en función de:

1. El número de personas afectadas, valorado en función del número potencial de víctimas mortales o heridos con lesiones graves y las consecuencias para la salud pública.

2. El impacto económico en función de la magnitud de las pérdidas económicas y el deterioro de productos y servicios.

3. El impacto medioambiental, degradación en el lugar y sus alrededores.

4. El impacto público y social, por la incidencia en la confianza de la población en la capacidad de las Administraciones Públicas, el sufrimiento físico y la alteración de la vida cotidiana, incluida la pérdida y el grave deterioro de servicios esenciales.

i) Análisis de riesgos: el estudio de las hipótesis de amenazas posibles necesario para determinar y evaluar las vulnerabilidades existentes en los diferentes sectores estratégicos y las posibles repercusiones de la perturbación o destrucción de las infraestructuras que le dan apoyo.

j) Interdependencias: los efectos que una perturbación en el funcionamiento de la instalación o servicio produciría en otras instalaciones o servicios, distinguiéndose las repercusiones en el propio sector y en otros sectores, y las repercusiones de ámbito local, autonómico, nacional o internacional.

k) Protección de infraestructuras críticas: el conjunto de actividades destinadas a asegurar la funcionalidad, continuidad e integridad de las infraestructuras críticas con el fin de prevenir, paliar y neutralizar el daño causado por un ataque deliberado contra dichas infraestructuras y a garantizar la integración de estas actuaciones con las demás que procedan de otros sujetos responsables dentro del ámbito de su respectiva competencia.

l) Información sensible sobre protección de infraestructuras estratégicas: los datos específicos sobre infraestructuras estratégicas que, de revelarse, podrían utilizarse para planear y llevar a cabo acciones cuyo objetivo sea provocar la perturbación o la destrucción de éstas.

m) Operadores críticos: las entidades u organismos responsables de las inversiones o del funcionamiento diario de una instalación, red, sistema, o equipo físico o de tecnología de la información designada como infraestructura crítica con arreglo a la presente Ley.

n) Nivel de Seguridad: aquel cuya activación por el Ministerio del Interior está previsto en el Plan Nacional de Protección de Infraestructuras Críticas, de acuerdo con la evaluación general de la amenaza y con la específica que en cada supuesto se efectúe sobre cada infraestructura, en virtud del cual corresponderá declarar un grado concreto de intervención de los diferentes organismos responsables en materia de seguridad.

o) Catálogo Nacional de Infraestructuras Estratégicas: la información completa, actualizada, contrastada e informáticamente sistematizada relativa a las características específicas de cada una de las infraestructuras estratégicas existentes en el territorio nacional.

Artículo 3. *Ámbito de aplicación.*

1. La presente Ley se aplicará a las infraestructuras críticas ubicadas en el territorio nacional vinculadas a los sectores estratégicos definidos en el anexo de esta Ley.
2. Se exceptúan de su aplicación las infraestructuras dependientes del Ministerio de Defensa y de las Fuerzas y Cuerpos de Seguridad, que se regirán, a efectos de control administrativo, por su propia normativa y procedimientos.
3. La aplicación de esta Ley se efectuará sin perjuicio de:

a) La misión y funciones del Centro Nacional de Inteligencia establecidas en su normativa específica, contando siempre con la necesaria colaboración y complementariedad con aquéllas.
b) Los criterios y disposiciones contenidos en la Ley 25/1964, de 29 de abril, sobre energía nuclear, y normas de desarrollo de la misma, y en la Ley 15/1980, de 22 de abril, de creación del Consejo de Seguridad Nuclear, reformada por la Ley 33/2007, de 7 de noviembre.
c) Lo previsto en el Programa Nacional de Seguridad de la Aviación Civil contemplado en la Ley 21/2003, de 7 de julio, de Seguridad Aérea, y su normativa complementaria.

Artículo 4. *El Catálogo Nacional de Infraestructuras Estratégicas.*

1. El Ministerio del Interior, a través de la Secretaría de Estado de Seguridad, será el responsable del Catálogo Nacional de Infraestructuras Estratégicas (en adelante, el Catálogo), instrumento que contendrá toda la información y valoración de las infraestructuras estratégicas del país, entre las que se hallarán incluidas aquellas clasificadas como Críticas o Críticas Europeas, en las condiciones que se determinen en el Reglamento que desarrolle la presente Ley.
2. La competencia para clasificar una infraestructura como estratégica, y en su caso, como infraestructura crítica o infraestructura crítica europea, así como para incluirla en el Catálogo Nacional de Infraestructuras Estratégicas, corresponderá al Ministerio del Interior, a través de la Secretaria de Estado de Seguridad, incluidas las propuestas, en su caso, del órgano competente de las Comunidades Autónomas y Ciudades con Estatuto de Autonomía que ostenten competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público en relación con las infraestructuras ubicadas en su demarcación territorial.

TÍTULO II

El Sistema de Protección de Infraestructuras Críticas

Artículo 5. *Finalidad.*

1. El Sistema de Protección de Infraestructuras Críticas (en adelante, el Sistema) se compone de una serie de instituciones, órganos y empresas, procedentes tanto del sector público como del privado, con responsabilidades en el correcto funcionamiento de los servicios esenciales o en la seguridad de los ciudadanos.
2. Son agentes del Sistema, con las funciones que se determinen reglamentariamente, los siguientes:

a) La Secretaría de Estado de Seguridad del Ministerio del Interior.
b) El Centro Nacional para la Protección de las Infraestructuras Críticas.
c) Los Ministerios y organismos integrados en el Sistema, que serán los incluidos en el anexo de esta Ley.
d) Las Comunidades Autónomas y las Ciudades con Estatuto de Autonomía.

e) Las Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía.

f) Las Corporaciones Locales, a través de la asociación de Entidades Locales de mayor implantación a nivel nacional.

g) La Comisión Nacional para la Protección de las Infraestructuras Críticas.

h) El Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas.

i) Los operadores críticos del sector público y privado.

Artículo 6. *La Secretaría de Estado de Seguridad.*

La Secretaría de Estado de Seguridad es el órgano superior del Ministerio del Interior responsable del Sistema de Protección de las infraestructuras críticas nacionales.

Para el desempeño de su cometido, el Reglamento de desarrollo de esta Ley determinará sus competencias en la materia, que ejercerá con la asistencia de los demás integrantes del Sistema y, principalmente, del Centro Nacional para la Protección de las Infraestructuras Críticas.

Artículo 7. *El Centro Nacional para la Protección de las Infraestructuras Críticas.*

1. Se crea el Centro Nacional para la Protección de las Infraestructuras Críticas (en adelante, el CNPIC) como órgano ministerial encargado del impulso, la coordinación y supervisión de todas las actividades que tiene encomendadas la Secretaría de Estado de Seguridad en relación con la protección de las Infraestructuras Críticas en el territorio nacional.

2. El CNPIC dependerá orgánicamente de la Secretaría de Estado de Seguridad, y sus funciones serán las que reglamentariamente se establezcan.

3. Sin perjuicio de lo dispuesto en el apartado anterior, corresponderá al CNPIC la realización de altas, bajas y modificaciones de infraestructuras en el Catálogo, así como la determinación de la criticidad de las infraestructuras estratégicas incluidas en el mismo.

Artículo 8. *Ministerios y organismos integrados en el Sistema de Protección de Infraestructuras Críticas.*

1. Por cada sector estratégico, se designará, al menos, un ministerio, organismo, entidad u órgano de la Administración General del Estado integrado en el Sistema. El nombramiento, alta o baja en éste de un ministerio u organismo con responsabilidad sobre un sector estratégico se efectuará mediante la modificación del anexo de la presente Ley.

2. Los ministerios y organismos del Sistema serán los encargados de impulsar, en el ámbito de sus competencias, las políticas de seguridad del Gobierno sobre los distintos sectores estratégicos nacionales y de velar por su aplicación, actuando igualmente como puntos de contacto especializados en la materia. Para ello, colaborarán con el Ministerio del Interior a través de la Secretaría de Estado de Seguridad.

3. Con tales objetivos, los ministerios y organismos del Sistema desempeñarán las funciones que reglamentariamente se determinen.

4. Un ministerio u organismo del Sistema podrá tener competencias, igualmente, sobre dos o más sectores estratégicos, conforme a lo establecido en el anexo de la presente Ley.

Artículo 9. *Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía.*

1. Los Delegados del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía tendrán, bajo la autoridad del Secretario de Estado de Seguridad, y en el ejercicio de sus competencias, una serie de facultades respecto de las infraestructuras críticas localizadas en su demarcación.

2. El desarrollo reglamentario de dichas facultades en todo caso incluirá la intervención, a través de las Fuerzas y Cuerpos de Seguridad, en la implantación de los diferentes Planes de Protección Específico y de Apoyo Operativo, así como la propuesta a la Secretaría de Estado de Seguridad de la declaración de una zona como crítica.

3. No obstante lo dispuesto en el apartado primero de este artículo, las Comunidades Autónomas con competencias estatutariamente reconocidas para la protección de bienes y personas y el mantenimiento del orden público desarrollarán, sobre las infraestructuras ubicadas en su territorio, aquellas facultades de las Delegaciones del Gobierno relativas a la coordinación de los cuerpos policiales autonómicos y, en su caso, a la activación por aquellos del Plan de Apoyo Operativo que corresponda para responder ante una alerta de seguridad.

Artículo 10. *Comunidades Autónomas y Ciudades con Estatuto de Autonomía.*

1. Las Comunidades Autónomas y Ciudades con Estatuto de Autonomía que ostenten competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público podrán desarrollar, sobre las infraestructuras ubicadas en su demarcación territorial, las facultades que reglamentariamente se determinen respecto a su protección, sin perjuicio de los mecanismos de coordinación que se establezcan.

2. En todo caso, las Comunidades Autónomas mencionadas en el apartado anterior participarán en el proceso de declaración de una zona como crítica, en la aprobación del Plan de Apoyo Operativo que corresponda, y en las reuniones del Grupo de Trabajo Interdepartamental. Asimismo, serán miembros de la Comisión Nacional para la Protección de las Infraestructuras Críticas.

3. Las Comunidades Autónomas no incluidas en los apartados anteriores participarán en el Sistema de Protección de Infraestructuras Críticas y en los Órganos previstos en esta Ley, de acuerdo con las competencias que les reconozcan sus respectivos Estatutos de Autonomía.

Artículo 11. *Comisión Nacional para la Protección de las Infraestructuras Críticas.*

1. Se crea la Comisión Nacional para la Protección de las Infraestructuras Críticas (en adelante, la Comisión) como órgano colegiado adscrito a la Secretaría de Estado de Seguridad.

2. La Comisión será la competente para aprobar los diferentes Planes Estratégicos Sectoriales así como para designar a los operadores críticos, a propuesta del Grupo de Trabajo Interdepartamental para la Protección de Infraestructuras Críticas.

3. Sus funciones y composición serán las que reglamentariamente se establezcan.

Artículo 12. *Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas.*

1. El Sistema contará con un Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas (en adelante, el Grupo de Trabajo), cuya composición y funciones se determinarán reglamentariamente.

2. Le corresponderá, en todo caso, la elaboración de los diferentes Planes Estratégicos Sectoriales y la propuesta a la Comisión de la designación de los operadores críticos por cada uno de los sectores estratégicos definidos.

Artículo 13. *Operadores críticos.*

1. Los operadores considerados críticos en virtud de esta Ley deberán colaborar con las autoridades competentes del Sistema, con el fin de optimizar la protección de las infraestructuras críticas y de las infraestructuras críticas europeas por ellos gestionados. Con ese fin, deberán:

a) Asesorar técnicamente al Ministerio del Interior, a través del CNPIC, en la valoración de las infraestructuras propias que se aporten al Catálogo, actualizando los datos disponibles con una periodicidad anual y, en todo caso, a requerimiento del citado Ministerio.

b) Colaborar, en su caso, con el Grupo de Trabajo en la elaboración de los Planes Estratégicos Sectoriales y en la realización de los análisis de riesgos sobre los sectores estratégicos donde se encuentren incluidos.

c) Elaborar el Plan de Seguridad del Operador en los términos y con los contenidos que se determinen reglamentariamente, debiendo acreditar la implantación de las medidas exigidas por la autoridad competente a través de la certificación oportuna.

d) Elaborar, según se disponga reglamentariamente, un Plan de Protección Específico por cada una de las infraestructuras consideradas como críticas en el Catálogo, debiendo acreditar la implantación de las medidas exigidas por la autoridad competente a través de la certificación oportuna.

e) Designar a un Responsable de Seguridad y Enlace en los términos de la presente Ley.

f) Designar a un Delegado de Seguridad por cada una de sus infraestructuras consideradas Críticas o Críticas Europeas por el Ministerio del Interior, comunicando su designación a los órganos correspondientes.

g) Facilitar las inspecciones que las autoridades competentes lleven a cabo para verificar el cumplimiento de la normativa sectorial y adoptar las medidas de seguridad que sean precisas en cada Plan, solventando en el menor tiempo posible las deficiencias encontradas.

h) Constituir un Área de Seguridad del Operador, de la manera que reglamentariamente se determine

2. Será requisito para la designación de los operadores críticos, tanto del sector público como del privado, que al menos una de las infraestructuras que gestionen reúna la consideración de Infraestructura Crítica, mediante la correspondiente propuesta de la que, en todo caso, el CNPIC informará al operador antes de proceder a su clasificación definitiva.

3. La designación como tales de los operadores críticos en cada uno de los sectores o subsectores estratégicos definidos se efectuará en los términos que reglamentariamente se establezcan.

4. Los operadores críticos tendrán en el CNPIC el punto directo de interlocución con el Ministerio del Interior en lo relativo a sus responsabilidades, funciones y obligaciones. En el caso de que los operadores críticos del Sector Público estén vinculados o dependan de una Administración Pública, el órgano competente de ésta podrá erigirse, a través del CNPIC, en el interlocutor con el Ministerio del Interior.

TÍTULO III

Instrumentos y comunicación del Sistema

Artículo 14. *Instrumentos de planificación del Sistema.*

1. La Protección de las Infraestructuras Críticas frente a las eventuales amenazas que puedan ponerlas en situación de riesgo requiere la adopción y aplicación de los siguientes planes de actuación:

a) El Plan Nacional de Protección de las Infraestructuras Críticas.
b) Los Planes Estratégicos Sectoriales.
c) Los Planes de Seguridad del Operador.
d) Los Planes de Protección Específicos.
e) Los Planes de Apoyo Operativo.

2. El Ministerio del Interior, a través de la Secretaría de Estado de Seguridad, elaborará el Plan Nacional de Protección de las Infraestructuras Críticas, siendo éste el documento estructural que permitirá dirigir y coordinar las actuaciones precisas para proteger las infraestructuras críticas en la lucha contra el terrorismo.

3. Los Planes Estratégicos Sectoriales serán asimismo elaborados por el Grupo de Trabajo y aprobados por la Comisión, e incluirán, por sectores, los criterios definidores de las medidas a adoptar para hacer frente a una situación de riesgo.

4. Los Planes de Seguridad del Operador y los Planes de Protección Específicos deberán ser elaborados por los operadores críticos respecto a todas sus infraestructuras clasificadas como Críticas o Críticas Europeas. Se trata de instrumentos de planificación a través de los cuales aquéllos asumen la obligación de colaborar en la identificación de dichas infraestructuras, especificar las políticas a implementar en materia de seguridad de las mismas, así como implantar las medidas generales de protección, tanto las permanentes

como aquellas de carácter temporal que, en su caso, vayan a adoptar para prevenir, proteger y reaccionar ante posibles ataques deliberados contra aquéllas.

5. Los Planes de Apoyo Operativo deberán ser elaborados por el Cuerpo Policial estatal o, en su caso, autonómico, con competencia en la demarcación, para cada una de las infraestructuras clasificadas como Críticas o Críticas Europeas dotadas de un Plan de Protección Específico, debiendo contemplar las medidas de vigilancia, prevención, protección o reacción a prestar, de forma complementaria a aquellas previstas por los operadores críticos.

6. El contenido concreto y el procedimiento de elaboración, aprobación y registro de cada uno de los planes serán los que se determinen reglamentariamente.

Artículo 15. *Seguridad de las comunicaciones.*

1. La Secretaría de Estado de Seguridad arbitrará los sistemas de gestión que permitan una continua actualización y revisión de la información disponible en el Catálogo por parte del CNPIC, así como su difusión a los organismos autorizados.

2. Las Administraciones Públicas velarán por la garantía de la confidencialidad de los datos sobre infraestructuras estratégicas a los que tengan acceso y de los planes que para su protección se deriven, según la clasificación de la información almacenada.

3. Los sistemas, las comunicaciones y la información referida a la protección de las infraestructuras críticas contarán con las medidas de seguridad necesarias que garanticen su confidencialidad, integridad y disponibilidad, según el nivel de clasificación que les sea asignado.

Artículo 16. *El Responsable de Seguridad y Enlace.*

1. Los operadores críticos nombrarán y comunicarán al Ministerio del Interior un Responsable de Seguridad y Enlace con la Administración en el plazo que reglamentariamente se establezca.

2. En todo caso, el Responsable de Seguridad y Enlace designado deberá contar con la habilitación de Director de Seguridad expedida por el Ministerio del Interior según lo previsto en la normativa de seguridad privada o con la habilitación equivalente, según su normativa específica.

3. Las funciones específicas del Responsable de Seguridad y Enlace serán las previstas reglamentariamente.

Artículo 17. *El Delegado de Seguridad de la Infraestructura Crítica.*

1. Los operadores con Infraestructuras consideradas Críticas o Críticas Europeas por el Ministerio del Interior comunicarán a las Delegaciones del Gobierno o, en su caso, al órgano competente de la Comunidad Autónoma con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público donde aquéllas se ubiquen, la existencia de un Delegado de Seguridad para dicha infraestructura.

2. El plazo para efectuar dicha comunicación, así como las funciones específicas del Delegado de Seguridad de la Infraestructura Crítica, serán los que reglamentariamente se establezcan.

Artículo 18. *Seguridad de los datos clasificados.*

El operador crítico deberá garantizar la seguridad de los datos clasificados relativos a sus propias infraestructuras, mediante los medios de protección y los sistemas de información adecuados que reglamentariamente se determinen.

Disposición adicional primera. *Normativa y régimen económico aplicable a la Comisión Nacional para la Protección de las Infraestructuras Críticas y al Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas.*

En lo no previsto en la presente Ley, se estará a lo dispuesto para el funcionamiento de los órganos colegiados en el Capítulo II del Título II de la Ley 30/1992, de 26 de noviembre, de Régimen jurídico de las Administraciones Públicas y del Procedimiento Administrativo

Común. Así mismo, el funcionamiento y los trabajos de la Comisión, así como del Grupo de Trabajo previstos en la presente norma se llevarán a cabo con cargo a las dotaciones presupuestarias y los medios personales y tecnológicos del Ministerio del Interior, sin que supongan incremento alguno del gasto público.

Disposición adicional segunda. *Clasificación de los Planes.*

Los Planes a los que se refiere el artículo 14 de la presente Ley tendrán la clasificación que les corresponda en virtud de la normativa vigente en la materia, la cual deberá constar de forma expresa en el instrumento de su aprobación.

Disposición adicional tercera. *Fuerzas y Cuerpos de Seguridad.*

Las referencias efectuadas en la presente Ley a las Fuerzas y Cuerpos de Seguridad incluyen, en todo caso, a los Cuerpos policiales dependientes de las Comunidades Autónomas con competencias estatutarias reconocidas para la protección de personas y bienes y para el mantenimiento del orden público.

Disposición adicional cuarta. *Ceuta y Melilla.*

De conformidad con lo establecido en los Estatutos de Autonomía de las Ciudades de Ceuta y Melilla, los Consejos de Gobierno de ambas, de acuerdo con la Delegación del Gobierno respectiva, podrán emitir informes y propuestas en relación con la adopción de medidas específicas sobre las infraestructuras situadas en ellas que sean objeto de la presente Ley.

Disposición final primera. *Título competencial.*

Esta Ley se dicta al amparo de la competencia atribuida al Estado en virtud del artículo 149.1.29.ª de la Constitución Española en materia de seguridad pública.

Disposición final segunda. *Competencias en materia de Protección Civil.*

Lo dispuesto en esta Ley se entiende sin perjuicio de lo que establezca la normativa autonómica en materia de protección civil, de acuerdo con las competencias correspondientes a cada territorio en virtud de lo dispuesto en los correspondientes Estatutos de Autonomía.

Disposición final tercera. *Incorporación de Derecho comunitario.*

Mediante esta Ley y sus ulteriores desarrollos reglamentarios se incorpora al Derecho español la Directiva 2008/114/CE del Consejo, de 8 de diciembre, sobre la identificación y clasificación de Infraestructuras Críticas Europeas y la evaluación de la necesidad de mejorar su protección.

Disposición final cuarta. *Habilitación para el desarrollo reglamentario.*

1. Se habilita al Gobierno para que en plazo de seis meses dicte el Reglamento de la presente Ley.
2. Igualmente se habilita al Gobierno a modificar por Real Decreto, a propuesta del titular del Ministerio del Interior y del titular del Departamento competente por razón de la materia, el Anexo de esta Ley.
3. En el ámbito de sus competencias, las Comunidades Autónomas podrán igualmente elaborar las normas reglamentarias necesarias para el desarrollo de la presente Ley.

Disposición final quinta. *Entrada en vigor.*

La presente Ley entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

ANEXO

Sectores estratégicos y Ministerios/Organismos del sistema competentes

Sector	Ministerio/Organismo del sistema
Administración.	Ministerio Presidencia.
	Ministerio Interior.
	Ministerio Defensa.
	Centro Nacional de Inteligencia.
	Ministerio Política Territorial y Administración Pública.
Espacio.	Ministerio Defensa.
Industria nuclear.	Ministerio Industria, Turismo y Comercio.
	Consejo de Seguridad Nuclear.
Industria química.	Ministerio Interior.
Instalaciones de investigación.	Ministerio Ciencia e Innovación.
	Ministerio Medio Ambiente, y Medio Rural y Marino.
Agua.	Ministerio Medio Ambiente, y Medio Rural y Marino.
	Ministerio Sanidad, Política Social e Igualdad.
Energía.	Ministerio Industria, Turismo y Comercio.
Salud.	Ministerio Sanidad, Política Social e Igualdad.
	Ministerio Ciencia e Innovación.
Tecnologías de la Información y las Comunicaciones (TIC).	Ministerio Industria, Turismo y Comercio.
	Ministerio Defensa.
	Centro Nacional de Inteligencia.
	Ministerio Ciencia e Innovación.
	Ministerio Política Territorial y Administración Pública.
Transporte.	Ministerio Fomento.
Alimentación.	Ministerio Medio Ambiente, y Medio Rural y Marino.
	Ministerio Sanidad, Política Social e Igualdad.
	Ministerio Industria, Turismo y Comercio.
Sistema financiero y tributario.	Ministerio Economía y Hacienda.

§ 23

Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas

Ministerio del Interior
«BOE» núm. 121, de 21 de mayo de 2011
Última modificación: sin modificaciones
Referencia: BOE-A-2011-8849

La Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas habilita al Gobierno, en su disposición final cuarta, para dictar el Reglamento de ejecución de desarrollo de la mencionada Ley.

En cumplimiento de este mandato, el presente real decreto se aprueba, en primer lugar, con la finalidad de desarrollar, concretar y ampliar los aspectos contemplados en la citada Ley, máxime cuando del tenor de la misma se desprende no sólo la articulación de un complejo Sistema de carácter interdepartamental para la protección de las infraestructuras críticas, compuesto por órganos y entidades tanto de las Administraciones Públicas como del sector privado, sino el diseño de todo un planeamiento orientado a prevenir y proteger las denominadas infraestructuras críticas de las amenazas o actos intencionados provenientes de figuras delictivas como el terrorismo, potenciados a través de las tecnologías de la comunicación.

En segundo lugar, este texto normativo no sólo es coherente con el marco legal del que trae causa, sino que además sirve a los fines del Sistema Nacional de Gestión de Situaciones de Crisis y cumple con la transposición obligatoria de la Directiva 2008/114/CE, del Consejo de la Unión Europea, de 8 de diciembre, en vigor desde el 12 de enero de 2009, sobre la identificación y designación de Infraestructuras Críticas Europeas y la evaluación de la necesidad de mejorar su protección. A ello obedecen las amplias previsiones que el texto contempla en el ámbito de los diferentes Planes que deben elaborar tanto las Administraciones Públicas –en el caso del Plan Nacional de Protección de las Infraestructuras Críticas, los Planes Estratégicos Sectoriales y los Planes de Apoyo Operativo– como las empresas, organizaciones o instituciones clasificadas como operadores críticos, a quienes la Ley asigna una serie de obligaciones, entre las que se encuentran la elaboración de sendos instrumentos de planificación: los Planes de Seguridad del Operador y los Planes de Protección Específicos.

Asimismo, la Ley prevé que los operadores críticos designen a un Responsable de Seguridad y Enlace –a quien se exige la habilitación de director de seguridad que concede el Ministerio del Interior al personal de seguridad de las empresas de Seguridad Privada en virtud de lo dispuesto en el Real Decreto 2364/1994, de 9 de diciembre, por el que se aprueba el Reglamento de Seguridad Privada, o habilitación equivalente, según su normativa específica–. Igualmente, se contempla la designación de un Delegado de Seguridad por cada una de las infraestructuras críticas identificadas.

En lo que a su contenido se refiere, el presente real decreto consta de un artículo único, una disposición transitoria única y dos disposiciones finales. Por su parte, el Reglamento consta de 36 artículos estructurados en cuatro Títulos. El Título I contiene las cuestiones generales relativas a su objeto y ámbito de aplicación, y dedica un artículo a la figura del Catálogo Nacional de Infraestructuras Estratégicas, como instrumento de la Secretaría de Estado de Seguridad del Ministerio del Interior que debe aglutinar todos los datos y la valoración de la criticidad de las citadas infraestructuras y que será empleado como base para planificar las actuaciones necesarias en materia de seguridad y protección de las mismas, al nutrirse de las aportaciones de los propios operadores. El Título II está plenamente dedicado al Sistema de Protección de Infraestructuras Críticas, y desarrolla, entre otras, las previsiones legales relativas a los órganos creados por la Ley, esto es, el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC), la Comisión Nacional para la Protección de las Infraestructuras Críticas y el Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas, concretando la composición, competencias y funcionamiento de todos ellos. El Título III se encarga de la regulación de los instrumentos de planificación, centrándose en cada uno de los Planes antes citados, cuyo proceso de elaboración, aprobación y registro, así como sus contenidos materiales, regula con mayor detalle. Finalmente, el Título IV está consagrado a la seguridad de las comunicaciones y a las figuras del Responsable de Seguridad y Enlace y del Delegado de Seguridad de la infraestructura crítica.

La tramitación del presente real decreto ha sido fruto de un intenso diálogo y colaboración entre los distintos Departamentos Ministeriales y organismos afectados, contando también con la aportación de las distintas Comunidades Autónomas y del sector empresarial, tras el trámite de información pública otorgado a todos ellos, lo que ha contribuido a dotar al texto de un extenso y, por otro lado, imprescindible, grado de consenso.

En su virtud, a propuesta del Vicepresidente Primero del Gobierno y Ministro del Interior, con la aprobación previa del Vicepresidente Tercero del Gobierno y Ministro de Política Territorial y Administración Pública, con el informe favorable de la Vicepresidenta Segunda del Gobierno y Ministra de Economía y Hacienda, de acuerdo con el Consejo de Estado, y previa deliberación del Consejo de Ministros en su reunión del día 20 de mayo de 2011,

DISPONGO:

TÍTULO I

Artículo único. *Aprobación del Reglamento de Protección de las infraestructuras críticas.*

En desarrollo y ejecución de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, se aprueba el Reglamento de Protección de las Infraestructuras Críticas, cuyo texto se inserta a continuación.

Disposición transitoria única. *Unidades y puestos de trabajo con nivel orgánico inferior a Subdirección General.*

Las unidades y puestos de trabajo con nivel orgánico inferior a Subdirección General del Centro Nacional para la Protección de las Infraestructuras Críticas continuarán subsistentes y serán retribuidos con cargo a los mismos créditos presupuestarios, hasta que se aprueben las relaciones de puestos de trabajo adaptadas a la estructura organizativa proyectada en el ámbito de la protección de las infraestructuras críticas. Dicha adaptación en ningún caso podrá generar incremento de gasto público.

Disposición final primera. *Título competencial.*

Este real decreto se dicta al amparo de la competencia atribuida al Estado en materia de seguridad pública en el artículo 149.1.29.ª de la Constitución.

Disposición final segunda. *Entrada en vigor.*

El presente real decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

REGLAMENTO DE PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS

TÍTULO I

Disposiciones generales

CAPÍTULO I

Objeto y ámbito de aplicación

Artículo 1. *Objeto.*

1. El presente reglamento tiene por objeto desarrollar el marco previsto en la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, a fin de concretar las actuaciones de los distintos órganos integrantes del Sistema de Protección de Infraestructuras Críticas (en adelante, el Sistema) así como los diferentes instrumentos de planificación del mismo.

2. Asimismo, regula las especiales obligaciones que deben asumir tanto el Estado como los operadores de aquellas infraestructuras que se determinen como críticas, según lo dispuesto en el artículo 2, párrafos e) y f) de la citada Ley.

Artículo 2. *Ámbito de aplicación.*

El ámbito de aplicación del presente reglamento será el previsto por el artículo 3 de la Ley 8/2011, de 28 de abril.

CAPÍTULO II

El Catálogo Nacional de Infraestructuras Estratégicas

Artículo 3. *El Catálogo Nacional de Infraestructuras Estratégicas.*

1. El Catálogo Nacional de infraestructuras estratégicas (en adelante, el Catálogo) es el registro de carácter administrativo que contiene información completa, actualizada y contrastada de todas las infraestructuras estratégicas ubicadas en el territorio nacional, incluyendo las críticas así como aquéllas clasificadas como críticas europeas que afecten a España, con arreglo a la Directiva 2008/114/CE.

2. La finalidad principal del Catálogo es valorar y gestionar los datos disponibles de las diferentes infraestructuras, con el objetivo de diseñar los mecanismos de planificación, prevención, protección y reacción ante una eventual amenaza contra aquéllas y, en caso de ser necesario, activar, conforme a lo previsto por el Plan Nacional de Protección de las Infraestructuras Críticas, una respuesta ágil, oportuna y proporcionada, de acuerdo con el nivel y características de la amenaza de que se trate.

Artículo 4. *Contenido del Catálogo.*

1. En el Catálogo deberán incorporarse, entre otros datos, los relativos a la descripción de las infraestructuras, su ubicación, titularidad y administración, servicios que prestan, medios de contacto, nivel de seguridad que precisan en función de los riesgos evaluados así como la información obtenida de las Fuerzas y Cuerpos de Seguridad.

2. El Catálogo se nutrirá de la información que le faciliten al Centro Nacional para la Protección de las Infraestructuras Críticas (en adelante, CNPIC) los operadores de las infraestructuras así como el resto de sujetos responsables del Sistema relacionados en el artículo 5 de la Ley 8/2011, de 28 de abril.

3. El Catálogo Nacional de Infraestructuras Estratégicas tiene, conforme a lo dispuesto en la legislación vigente en materia de secretos oficiales, la calificación de SECRETO, conferida por Acuerdo de Consejo de Ministros de 2 de noviembre de 2007, calificación que comprende, además de los datos contenidos en el propio Catálogo, los equipos, aplicaciones informáticas y sistemas de comunicaciones inherentes al mismo, así como el nivel de habilitación de las personas que pueden acceder a la información en él contenida.

Artículo 5. *Gestión y actualización del Catálogo.*

1. La custodia, gestión y mantenimiento del Catálogo Nacional de infraestructuras estratégicas corresponde al Ministerio del Interior, a través de la Secretaría de Estado de Seguridad.

2. El Ministerio del Interior, a través de la Secretaría de Estado de Seguridad, será responsable de clasificar una infraestructura como estratégica y, en su caso, como infraestructura crítica o infraestructura crítica europea, así como de incluirla por vez primera en el Catálogo, previa comprobación de que cumple uno o varios de los criterios horizontales de criticidad previstos en el artículo 2, apartado h) de la Ley 8/2011, de 28 de abril.

3. El proceso de identificación de una infraestructura como crítica se realizará por el CNPIC, que podrá recabar la participación y el asesoramiento del interesado, así como de los agentes del Sistema competentes, a los que informará posteriormente del resultado de tal proceso.

4. La clasificación de una infraestructura como crítica europea supondrá la obligación adicional de comunicar su identidad a otros Estados miembros que puedan verse afectados de forma significativa por aquélla, de acuerdo con lo previsto por la Directiva 2008/114/CE. En tal caso, las notificaciones, en reciprocidad con otros Estados miembros, se realizarán por el CNPIC, de acuerdo con la clasificación de seguridad que corresponda según la normativa vigente.

5. En los casos en que se produzca una modificación relevante que afecte a las infraestructuras inscritas y que sea de interés a los efectos previstos en el presente reglamento, los operadores críticos responsables de las mismas facilitarán, a través de los medios puestos a su disposición por el Ministerio del Interior, los nuevos datos de aquéllas al CNPIC, que deberá validarlos con carácter previo a su incorporación al Catálogo. En todo caso, la actualización de los datos disponibles deberá hacerse con periodicidad anual.

TÍTULO II

Los agentes del Sistema de Protección de Infraestructuras Críticas

Artículo 6. *La Secretaría de Estado de Seguridad.*

La Secretaría de Estado de Seguridad es el órgano superior del Ministerio del Interior responsable del Sistema de Protección de las Infraestructuras Críticas Nacionales, para lo cual su titular, u órgano en quien delegue, ejercerá las siguientes funciones:

a) Diseñar y dirigir la estrategia nacional de protección de infraestructuras críticas.

b) Aprobar el Plan Nacional de Protección de las Infraestructuras Críticas y dirigir su aplicación, declarando en su caso los niveles de seguridad a establecer en cada momento, conforme al contenido de dicho Plan y en coordinación con el Plan de Prevención y Protección Antiterrorista.

c) Aprobar los Planes de Seguridad de los Operadores y sus actualizaciones a propuesta del CNPIC, tomando en su caso, como referencia, las actuaciones del órgano u organismo competente para otorgar a aquéllos las autorizaciones correspondientes en virtud de su normativa sectorial.

d) Aprobar los diferentes Planes de Protección Específicos o las eventuales propuestas de mejora de éstos a propuesta del CNPIC, en los términos de lo dispuesto en el artículo 26 de este reglamento.

e) Aprobar los Planes de Apoyo Operativo, así como supervisar y coordinar la implantación de los mismos y de aquellas otras medidas de prevención y protección que

deban activarse tanto por las Fuerzas y Cuerpos de Seguridad y por las Fuerzas Armadas, en su caso, como por los propios responsables de seguridad de los operadores críticos.

f) Aprobar, previo informe del CNPIC, la declaración de una zona como crítica, a propuesta de las Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía o, en su caso, de las Comunidades Autónomas con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público.

g) Identificar los diferentes ámbitos de responsabilidad en la protección de infraestructuras críticas; analizando los mecanismos de prevención y respuesta previstos por cada uno de los actores implicados.

h) Emitir las instrucciones y protocolos de colaboración dirigidos tanto al personal y órganos ajenos al Ministerio del Interior como a los operadores de las infraestructuras estratégicas, así como fomentar la adopción de buenas prácticas.

i) Responder del cumplimiento de las obligaciones y compromisos asumidos por España en el marco de la Directiva 2008/114/CE, sin perjuicio de las competencias que corresponden al Ministerio de Asuntos Exteriores y de Cooperación.

j) Supervisar, dentro del ámbito de aplicación de este reglamento, los proyectos y estudios de interés y coordinar la participación en programas financieros y subvenciones procedentes de la Unión Europea.

k) Colaborar con los Ministerios y organismos integrados en el Sistema en la elaboración de toda norma sectorial que se dicte en desarrollo de la Ley 8/2011, de 28 de abril y del presente reglamento.

l) Cualesquiera otras funciones que, eventualmente, pudieran acordarse por la Comisión Delegada del Gobierno para Situaciones de Crisis.

Artículo 7. *El Centro Nacional para la Protección de las Infraestructuras Críticas.*

El CNPIC del Ministerio del Interior, orgánicamente dependiente de la Secretaría de Estado de Seguridad, tendrá el nivel orgánico que se determine en la correspondiente relación de puestos de trabajo, y desempeñará las siguientes funciones:

a) Asistir al Secretario de Estado de Seguridad en la ejecución de sus funciones en materia de protección de infraestructuras críticas, actuando como órgano de contacto y coordinación con los agentes del Sistema.

b) Ejecutar y mantener actualizado el Plan Nacional de Protección de las Infraestructuras Críticas conforme a lo previsto en el artículo 16 de este reglamento.

c) Determinar la criticidad de las infraestructuras estratégicas incluidas en el Catálogo.

d) Mantener operativo y actualizado el Catálogo, estableciendo los procedimientos de alta, baja y modificación de las infraestructuras, tanto nacionales como europeas, que en él se incluyan en virtud de los criterios horizontales y de los efectos de interdependencias sectoriales a partir de la información que le suministren los operadores y el resto de agentes del Sistema, así como establecer su clasificación interna.

e) Llevar a cabo las siguientes funciones respecto a los instrumentos de planificación previstos en este reglamento:

Dirigir y coordinar los análisis de riesgos que se realicen por los organismos especializados, públicos o privados, sobre cada uno de los sectores estratégicos en el marco de los Planes Estratégicos Sectoriales, para su estudio y deliberación por el Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas.

Establecer los contenidos mínimos de los Planes de Seguridad de los Operadores, de los Planes de Protección Específicos y de los Planes de Apoyo Operativo y supervisar el proceso de elaboración de éstos, recomendando, en su caso, el orden de preferencia de las contramedidas y los procedimientos a adoptar para garantizar su protección ante ataques deliberados.

Evaluar, tras la emisión de los correspondientes informes técnicos especializados, los Planes de Seguridad del Operador y proponerlos, en su caso, para su aprobación, al Secretario de Estado de Seguridad, u órgano en quien delegue.

Analizar los Planes de Protección Específicos facilitados por los operadores críticos respecto a las diferentes infraestructuras críticas o infraestructuras críticas europeas de su

titularidad y proponerlos, en su caso, para su aprobación, al Secretario de Estado de Seguridad, u órgano en quien delegue.

Validar los Planes de Apoyo Operativo diseñados para cada una de las infraestructuras críticas existentes en el territorio nacional por el Cuerpo Policial estatal o, en su caso, autonómico competente, previo informe, respectivamente, de las Delegaciones del Gobierno en las Comunidades Autónomas o de las Comunidades Autónomas que tengan competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público.

f) Elevar al Secretario de Estado de Seguridad, u órgano en quien delegue, las propuestas para la declaración de una zona como crítica que se efectúen.

g) Implantar, bajo el principio general de confidencialidad, mecanismos permanentes de información, alerta y comunicación con todos los agentes del Sistema.

h) Recopilar, analizar, integrar y valorar la información sobre infraestructuras estratégicas procedente de instituciones públicas, servicios policiales, operadores y de los diversos instrumentos de cooperación internacional para su remisión al Centro Nacional de Coordinación Antiterrorista del Ministerio del Interior o a otros organismos autorizados.

i) Participar en la realización de ejercicios y simulacros en el ámbito de la protección de las infraestructuras críticas.

j) Coordinar los trabajos y la participación de expertos en los diferentes grupos de trabajo y reuniones sobre protección de infraestructuras críticas, en los ámbitos nacional e internacional.

k) Ser, en el ámbito de la Protección de las Infraestructuras Críticas, el Punto Nacional de Contacto con organismos internacionales y con la Comisión Europea, así como elevar a ésta, previa consulta al Centro Nacional de Coordinación Antiterrorista, los informes sobre evaluación de amenazas y tipos de vulnerabilidades y riesgos encontrados en cada uno de los sectores en los que se hayan designado infraestructuras críticas europeas, en los plazos y condiciones marcados por la Directiva.

l) Ejecutar las acciones derivadas del cumplimiento de la Directiva 2008/114/CE en representación de la Secretaría de Estado de Seguridad.

Artículo 8. *Los Ministerios y organismos integrados en el Sistema de Protección de Infraestructuras Críticas.*

Los ministerios y organismos del Sistema a los que se refiere el artículo 8 de la Ley 8/2011, de 28 de abril tendrán las siguientes competencias:

a) Participar, a través del Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas, con el apoyo, en su caso, de los operadores, en la elaboración de los Planes Estratégicos Sectoriales, así como proceder a su revisión y actualización en los términos previstos en este reglamento.

b) Verificar, en el ámbito de sus competencias, el cumplimiento de los Planes Estratégicos Sectoriales y de las actuaciones derivadas de éstos, con excepción de las que se correspondan con medidas de seguridad concretas establecidas en infraestructuras específicas, o las que deban ser realizadas por otros órganos de la Administración General del Estado, conforme a su legislación específica.

c) Colaborar con la Secretaría de Estado de Seguridad tanto en la designación de los operadores críticos como en la elaboración de toda norma sectorial que se dicte en desarrollo de la Ley 8/2011, de 28 de abril, así como del presente reglamento.

d) Proporcionar asesoramiento técnico a la Secretaría de Estado de Seguridad en la catalogación de las infraestructuras dentro de su sector de competencia, poniendo a disposición del CNPIC en su caso la información técnica que ayude a determinar su criticidad, para su inclusión, exclusión o modificación en el Catálogo.

e) Custodiar, en los términos de la normativa sobre materias clasificadas y secretos oficiales, la información sensible sobre protección de infraestructuras estratégicas de la que dispongan en calidad de agentes del Sistema.

f) Designar a una persona para participar en los Grupos de Trabajo Sectoriales que, eventualmente, puedan crearse en el ámbito de la protección de infraestructuras críticas.

g) Participar, a solicitud del CNPIC o por iniciativa propia, en los diferentes grupos de trabajo y reuniones sobre protección de infraestructuras críticas relacionadas con su sector de coordinación, en los ámbitos nacional e internacional.

h) Colaborar con la Secretaría de Estado de Seguridad en las acciones derivadas del cumplimiento de la Directiva 2008/114/CE, conforme a lo dispuesto en el artículo 7, apartado l), de este reglamento.

i) Participar en el proceso de clasificación de una infraestructura como crítica, incluyendo el ejercicio de la facultad de propuesta a tal fin.

Artículo 9. *Las Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía.*

Bajo la autoridad del Secretario de Estado de Seguridad, y en el ejercicio de sus competencias, los Delegados del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía tendrán, respecto de las infraestructuras críticas localizadas en su territorio, las siguientes facultades:

a) Coordinar la actuación de las Fuerzas y Cuerpos de Seguridad del Estado ante una alerta de seguridad, y velar por la aplicación del Plan Nacional de Protección de Infraestructuras Críticas en caso de activación de éste.

b) Colaborar, en función de su ámbito territorial de actuación, con otros órganos de la Administración u organismos públicos competentes conforme a su legislación específica, así como con las delegaciones territoriales de otros ministerios y organismos del Sistema en las acciones que se desarrollen para el cumplimiento de los Planes Sectoriales vigentes en materia de protección de infraestructuras críticas.

c) Participar en la implantación de los diferentes Planes de Protección Específicos en aquellas infraestructuras críticas o infraestructuras críticas europeas existentes en su territorio, en los términos en los que se expresa el Capítulo IV del Título III de este reglamento.

d) Intervenir, a través del Cuerpo Policial estatal competente, y en colaboración con el responsable de seguridad de la infraestructura, en la implantación de los diferentes Planes de Apoyo Operativo en aquellas infraestructuras críticas o infraestructuras críticas europeas existentes en su territorio, conforme a lo establecido en el Capítulo V del Título III de este reglamento.

e) Proponer a la Secretaría de Estado de Seguridad a través del CNPIC la declaración de zona crítica sobre la base de la existencia de varias infraestructuras críticas o infraestructuras críticas europeas en una zona geográfica continua, con el fin de lograr una protección coordinada entre los diferentes operadores titulares y las Fuerzas y Cuerpos de Seguridad.

f) Custodiar la información sensible sobre protección de infraestructuras estratégicas de que dispongan en calidad de agentes del Sistema, en aplicación de la normativa vigente sobre materias clasificadas y secretos oficiales.

Artículo 10. *Las Comunidades Autónomas y las Ciudades con Estatuto de Autonomía.*

1. Las Comunidades Autónomas con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público desarrollarán, sobre las infraestructuras ubicadas en su territorio, las facultades previstas en los párrafos c), d, e) y f) del artículo anterior dada la existencia en ellas de Cuerpos policiales autonómicos, y sin perjuicio de que las respectivas Delegaciones del Gobierno en dichas Comunidades Autónomas tengan conocimiento de la información sensible y de los planes a que se refiere el presente reglamento.

2. En todo caso, la coordinación de las actuaciones que se lleven a cabo en materia de protección de las infraestructuras críticas entre las Fuerzas y Cuerpos de Seguridad del Estado y los Cuerpos policiales de las Comunidades Autónomas con competencias en materia de seguridad, se regirá por lo estipulado en los acuerdos de las Juntas de Seguridad correspondientes.

3. Las Comunidades Autónomas no incluidas en el apartado primero del presente artículo participarán en el Sistema y en los órganos colegiados del mismo de acuerdo con las competencias que les reconozcan sus respectivos Estatutos de Autonomía.

4. De acuerdo con lo dispuesto en sus Estatutos de Autonomía, las Ciudades de Ceuta y Melilla, a través de sus Consejos de Gobierno y de acuerdo con la Delegación de Gobierno respectiva, podrán emitir los oportunos informes y propuestas en relación con la adopción de medidas específicas sobre las infraestructuras críticas y críticas europeas situadas en su territorio.

Artículo 11. *La Comisión Nacional para la Protección de las Infraestructuras Críticas.*

1. La Comisión Nacional para la Protección de las Infraestructuras Críticas (en adelante, la Comisión) desempeñará las siguientes funciones:

a) Preservar, garantizar y promover la existencia de una cultura de seguridad de las infraestructuras críticas en el ámbito de las Administraciones públicas.

b) Promover la aplicación efectiva de las disposiciones de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas por parte de todos los sujetos responsables del sistema de protección de infraestructuras críticas, a partir de los informes emitidos al respecto por parte del Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas.

c) Llevar a cabo las siguientes actuaciones a propuesta del Grupo de Trabajo:

Aprobar los Planes Estratégicos Sectoriales.

Designar a los operadores críticos.

Aprobar la creación, modificación o supresión de grupos de trabajo sectoriales o de carácter técnico, estableciendo sus objetivos y sus marcos de actuación.

d) Impulsar aquéllas otras tareas que se estimen precisas en el marco de la cooperación interministerial para la protección de las infraestructuras críticas.

2. La Comisión será presidida por el Secretario de Estado de Seguridad, y sus miembros serán:

a) En representación del Ministerio del Interior:

El Director General de la Policía y de la Guardia Civil.

El Director General de Protección Civil y Emergencias.

El Director del CNPIC, que ejercerá las funciones de Secretario de la Comisión.

b) En representación del Ministerio de Defensa, el Director General de Política de Defensa.

c) En representación del Centro Nacional de Inteligencia, un Director General designado por el Secretario de Estado-Director de aquél.

d) En representación del Departamento de Infraestructura y Seguimiento para Situaciones de Crisis, su Director.

e) En representación del Consejo de Seguridad Nuclear, el Director Técnico de Protección Radiológica.

f) En representación de cada uno de los ministerios integrados en el Sistema, una persona con rango igual o superior a Director General, designada por el titular del Departamento ministerial correspondiente en razón del sector de actividad material que corresponda.

3. Además de los miembros mencionados en el apartado anterior, asistirá a las reuniones de la Comisión un representante con voz y voto por cada una de las Comunidades Autónomas que ostenten competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público. También participará, igualmente con voz y voto, un representante de la asociación de Entidades Locales de mayor implantación a nivel nacional en las reuniones.

En su caso, y cuando su presencia y criterio resulte imprescindible por razón de los temas a tratar, podrán ser convocados, por decisión de su presidente, organismos, expertos u otras Administraciones públicas.

4. La Comisión se reunirá al menos una vez al año, con carácter ordinario, y de forma extraordinaria cuando así se considere oportuno previa convocatoria de su Presidente, quien determinará el orden del día de la reunión en los términos previstos para los órganos colegiados en el Capítulo II del Título II de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. La secretaría de la Comisión radicará en el Director del CNPIC.

5. La Comisión será asistida por el Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas.

Artículo 12. *El Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas.*

1. El Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas (en adelante, el Grupo de Trabajo) desempeña las siguientes funciones:

a) Elaborar, con la colaboración de los agentes del Sistema afectados y el asesoramiento técnico pertinente, los diferentes Planes Estratégicos Sectoriales para su presentación a la Comisión, conforme a lo previsto en el Título III, Capítulo II, de este reglamento.

b) Proponer a la Comisión la designación de los operadores críticos por cada uno de los sectores estratégicos definidos.

c) Proponer a la Comisión la creación, modificación o supresión de grupos de trabajo sectoriales o de carácter técnico, supervisando, coordinando y efectuando el seguimiento de los mismos y de sus trabajos e informando oportunamente de los resultados obtenidos a la Comisión.

d) Efectuar los estudios y trabajos que, en el marco de este reglamento, le encomiende la Comisión. Para ello podrá contar, si es necesario, con el apoyo de personal técnico especializado.

2. El Grupo de Trabajo estará presidido por el Director del CNPIC, y estará compuesto por:

a) Un representante de cada uno de los ministerios del Sistema, designados por el titular del departamento ministerial correspondiente.

b) Un representante de la Dirección Adjunta Operativa del Cuerpo Nacional de Policía, designado por el titular de ésta.

c) Un representante de la Dirección Adjunta Operativa de la Guardia Civil, designado por el titular de aquélla.

d) Un representante de la Dirección General de Protección Civil y Emergencias del Ministerio del Interior, designado por el titular de ésta.

e) Un representante del Estado Mayor Conjunto de la Defensa, designado por el Jefe del Estado Mayor de la Defensa.

f) Un representante del Centro Nacional de Inteligencia, designado por el Secretario de Estado Director de dicho Centro.

g) Un representante del Departamento de Infraestructura y Seguimiento para Situaciones de Crisis, designado por el titular del Ministerio de la Presidencia u órgano en quien delegue, a propuesta del Director del Gabinete de la Presidencia del Gobierno.

h) Un representante del Consejo de Seguridad Nuclear, designado por el Presidente de dicho organismo.

i) Un representante del CNPIC, con funciones de Secretario.

3. Además de los miembros mencionados en el apartado anterior, asistirá a las reuniones del Grupo de Trabajo un representante, con voz y voto por cada una de las Comunidades Autónomas con competencias estatutariamente reconocidas para la protección de bienes y personas y para el mantenimiento del orden público. Asimismo, participará con voz y voto un representante de la asociación de Entidades Locales de mayor implantación a nivel nacional en las reuniones.

Por decisión de su presidente, podrán asistir aquellas otras Administraciones Públicas, organismos o expertos cuyo asesoramiento técnico se estime preciso en razón de los temas a tratar.

4. El Grupo de Trabajo se reunirá al menos dos veces al año, con carácter ordinario, y de forma extraordinaria cuando así se considere oportuno a convocatoria de su Presidente, quien determinará el orden del día de la reunión. La secretaría radicará en uno de los funcionarios que prestan servicios en el CNPIC, por decisión de su Director.

5. Para el ejercicio de las competencias que este reglamento atribuye al Grupo de Trabajo, podrán constituirse otros grupos de trabajo sectoriales para los sectores o subsectores incluidos en el anexo de la Ley 8/2011, de 28 de abril, en los que podrán participar, además del CNPIC y el correspondiente ministerio u organismo del Sistema, los operadores críticos y otros agentes del Sistema.

Artículo 13. *Operadores Críticos.*

1. Los operadores críticos serán los agentes integrantes del Sistema, que, procedentes tanto del sector público como del sector privado, reúnan las condiciones establecidas en el artículo 13 de la Ley 8/2011, de 28 de abril.

2. En aplicación de lo previsto en la citada Ley, corresponde a los operadores críticos:

a) Prestar su colaboración técnica a la Secretaría de Estado de Seguridad, a través del CNPIC, en la valoración de las infraestructuras propias que se aporten al Catálogo. Por ello, deberán actualizar los datos disponibles con una periodicidad anual y, en todo caso, a requerimiento o previa validación del CNPIC.

b) Colaborar, en su caso, con el Grupo de Trabajo, en la elaboración de los Planes Estratégicos Sectoriales y en la realización de los análisis de riesgos sobre los sectores estratégicos donde se encuentren incluidos.

c) Elaborar el Plan de Seguridad del Operador y proceder a su actualización periódicamente o cuando las circunstancias así lo exijan, conforme a lo que establece el Capítulo III, Título III del presente reglamento.

d) Elaborar un Plan de Protección Específico por cada una de las infraestructuras consideradas como críticas en el Catálogo así como proceder a su actualización periódicamente o cuando las circunstancias así lo exijan, conforme a lo establecido en el Capítulo IV, Título III del presente reglamento.

e) Designar a un Responsable de Seguridad y Enlace, en virtud de lo dispuesto en el artículo 34 del presente reglamento.

f) Designar a un Delegado de Seguridad por cada una de sus infraestructuras consideradas Críticas o Críticas Europeas por la Secretaría de Estado de Seguridad, comunicando su designación a los órganos correspondientes en virtud de lo dispuesto en el artículo 35 del presente reglamento.

g) Facilitar las inspecciones que las autoridades competentes lleven a cabo para verificar el cumplimiento de la normativa sectorial, en el marco de lo establecido en el Título III de este reglamento.

Artículo 14. *Designación de los operadores críticos.*

1. Para la designación de una empresa u organismo como operador crítico, bastará con que al menos una de las infraestructuras por él gestionadas reúna la consideración de infraestructura crítica, en aplicación de los criterios previstos en el artículo 2, apartado h), de la Ley 8/2011, de 28 de abril. En tal caso, el CNPIC, elaborará una propuesta de resolución y la notificará al titular o administrador de aquéllas.

2. La citada propuesta contendrá la intención de designar al titular o administrador de la instalación o instalaciones como operador crítico.

3. El interesado dispondrá de un plazo de quince días a contar desde el día siguiente a la recepción de la notificación para remitir al CNPIC las alegaciones que considere procedentes, transcurrido el cual la Comisión, a propuesta del Grupo de Trabajo, dictará la resolución en la que se designará, en su caso, a dicho operador, como crítico. Esta resolución podrá ser recurrida en alzada ante el Secretario de Estado de Seguridad, y, eventualmente, con posterioridad, ante la jurisdicción contencioso-administrativa, en los términos generales previstos en la legislación vigente en materia de procedimiento administrativo y del orden jurisdiccional contencioso-administrativo.

4. Las comunicaciones con el interesado tendrán en cuenta, en todo caso, la clasificación de seguridad que corresponda según la normativa vigente.

Artículo 15. *Interlocución con los operadores críticos.*

1. Los operadores críticos del Sector Privado tendrán en el CNPIC el punto directo de interlocución con la Secretaría de Estado de Seguridad en lo relativo a las responsabilidades, funciones y obligaciones recogidas en la Ley 8/2011, de 28 de abril, y en lo previsto este reglamento.

2. En aquellos casos en que los operadores críticos del Sector Público estén vinculados o dependan de una Administración pública, el órgano de dicha Administración que ostente competencias por razón de la materia podrá constituirse en el interlocutor con el Ministerio del Interior a través del CNPIC en lo relativo a las responsabilidades, funciones y obligaciones recogidas en la Ley 8/2011, de 28 de abril, y en lo previsto en este reglamento, debiendo comunicar dicha decisión al CNPIC.

TÍTULO III

Instrumentos de planificación

CAPÍTULO I

El Plan Nacional de Protección de las Infraestructuras Críticas

Artículo 16. *Finalidad, elaboración y contenido.*

1. El Plan Nacional de Protección de las Infraestructuras Críticas es el instrumento de programación del Estado elaborado por la Secretaría de Estado de Seguridad y dirigido a mantener seguras las infraestructuras españolas que proporcionan los servicios esenciales a la sociedad.

2. El Plan Nacional de Protección de las Infraestructuras Críticas establecerá los criterios y las directrices precisas para movilizar las capacidades operativas de las Administraciones públicas en coordinación con los operadores críticos, articulando las medidas preventivas necesarias para asegurar la protección permanente, actualizada y homogénea de nuestro sistema de infraestructuras estratégicas frente a las amenazas provenientes de ataques deliberados contra ellas.

3. Asimismo, el Plan preverá distintos niveles de seguridad e intervención policial, que se activarán, en cada caso, en función de los resultados de la evaluación de la amenaza y coordinadamente con el Plan de Prevención y Protección Antiterrorista en vigor, al cual deberá adaptarse.

Los distintos niveles de seguridad contendrán la adopción graduada de dispositivos y medidas de protección ante situaciones de incremento de la amenaza contra las infraestructuras estratégicas nacionales y requerirán el concurso de las Fuerzas y Cuerpos de Seguridad, las Fuerzas Armadas, en su caso, y los responsables de los organismos o titulares o gestores de las infraestructuras a proteger.

Artículo 17. *Aprobación, registro y clasificación.*

1. El Plan Nacional de Protección de las Infraestructuras Críticas será aprobado por resolución del titular de la Secretaría de Estado de Seguridad y quedará registrado en el CNPIC, sin perjuicio de que aquellos otros organismos que necesiten conocer del mismo sean autorizados para acceder a él por el Secretario de Estado de Seguridad.

2. El Plan estará clasificado conforme a lo que establece la legislación vigente en materia de secretos oficiales, debiendo constar expresamente tal clasificación en el instrumento de su aprobación.

Artículo 18. *Revisión y actualización.*

1. El Plan Nacional de Protección de las Infraestructuras Críticas será revisado cada cinco años por la Secretaría de Estado de Seguridad.
2. La modificación de alguno de los datos o instrucciones incluidos en el Plan Nacional de Protección de las Infraestructuras Críticas obligará a la automática actualización del mismo, que se llevará a cabo por el CNPIC y requerirá la aprobación expresa del Secretario de Estado de Seguridad.

CAPÍTULO II

Los Planes Estratégicos Sectoriales

Artículo 19. *Finalidad, elaboración y contenido.*

1. Los Planes Estratégicos Sectoriales son los instrumentos de estudio y planificación con alcance en todo el territorio nacional que permitirán conocer, en cada uno de los sectores contemplados en el anexo de la Ley 8/2011, de 28 de abril, cuáles son los servicios esenciales proporcionados a la sociedad, el funcionamiento general de éstos, las vulnerabilidades del sistema, las consecuencias potenciales de su inactividad y las medidas estratégicas necesarias para su mantenimiento.
2. El Grupo de Trabajo, coordinado por el CNPIC, elaborará con la participación y asesoramiento técnico de los operadores afectados, en su caso, un Plan Estratégico por cada uno de los sectores o subsectores de actividad que se determinen.
3. Los Planes Estratégicos Sectoriales estarán basados en un análisis general de riesgos donde se contemplen las vulnerabilidades y amenazas potenciales, tanto de carácter físico como lógico, que afecten al sector o subsector en cuestión en el ámbito de la protección de las infraestructuras estratégicas.
4. Cada Plan Estratégico Sectorial contendrá, como mínimo, los siguientes extremos:

a) Análisis de riesgos, vulnerabilidades y consecuencias a nivel global.
b) Propuestas de implantación de medidas organizativas y técnicas necesarias para prevenir, reaccionar y, en su caso, paliar, las posibles consecuencias de los diferentes escenarios que se prevean.
c) Propuestas de implantación de otras medidas preventivas y de mantenimiento (por ejemplo, ejercicios y simulacros, preparación e instrucción del personal, articulación de los canales de comunicación precisos, planes de evacuación o planes operativos para abordar posibles escenarios adversos).
d) Medidas de coordinación con el Plan Nacional de Protección de las Infraestructuras Críticas.

5. Los Planes Estratégicos Sectoriales podrán constituirse teniendo en cuenta otros planes o programas ya existentes, creados sobre la base de su propia legislación específica sectorial. Cuando los referidos planes o programas sectoriales reúnan los extremos a los que se refiere el apartado cuarto, podrán adoptarse los mismos como Plan Estratégico Sectorial del sector o subsector correspondiente.

Artículo 20. *Aprobación, registro y clasificación.*

1. Los Planes Estratégicos Sectoriales deberán ser aprobados por la Comisión en el plazo máximo de doce meses a partir de la entrada en vigor del presente real decreto.
2. El CNPIC gestionará y custodiará un registro central de todos los Planes Estratégicos Sectoriales existentes, una vez éstos sean aprobados por la Comisión. Los ministerios y organismos del Sistema tendrán acceso a los Planes de aquellos sectores para los que sean competentes.
3. Los Planes Estratégicos Sectoriales estarán clasificados conforme a lo que establece la legislación vigente en materia de secretos oficiales, debiendo constar expresamente en el instrumento de su aprobación. El CNPIC será responsable de garantizar a los agentes del Sistema autorizados el acceso a toda o parte de la información contenida en dichos planes.

Artículo 21. *Revisión y actualización.*

1. Los Planes Estratégicos Sectoriales deberán ser revisados cada dos años por los ministerios y organismos del Sistema.
2. La modificación de alguno de los datos incluidos en los Planes Estratégicos Sectoriales obligará a la automática actualización de éstos, que se llevará a cabo por los ministerios y organismos del Sistema que sean competentes en el sector afectado y será posteriormente aprobada por la Comisión.

CAPÍTULO III

Los Planes de Seguridad del Operador

Artículo 22. *Finalidad, elaboración y contenido.*

1. Los Planes de Seguridad del Operador son los documentos estratégicos definidores de las políticas generales de los operadores críticos para garantizar la seguridad del conjunto de instalaciones o sistemas de su propiedad o gestión.
2. En el plazo de seis meses a partir de la notificación de la resolución de su designación, cada operador crítico deberá haber elaborado un Plan de Seguridad del Operador y presentarlo al CNPIC, que lo evaluará y lo informará para su aprobación, si procede, por el Secretario de Estado de Seguridad u órgano en el que éste delegue.
3. Los Planes de Seguridad del Operador deberán establecer una metodología de análisis de riesgos que garantice la continuidad de los servicios proporcionados por dicho operador y en la que se recojan los criterios de aplicación de las diferentes medidas de seguridad que se implanten para hacer frente a las amenazas tanto físicas como lógicas identificadas sobre cada una de las tipologías de sus activos.
4. La Secretaría de Estado de Seguridad del Ministerio del Interior, a través del CNPIC, establecerá, con la colaboración de los Ministerios del Sistema y organismos dependientes, los contenidos mínimos de los Planes de Seguridad del Operador, así como el modelo en el que basar la elaboración de éstos.

Artículo 23. *Aprobación, registro y clasificación.*

1. El Secretario de Estado de Seguridad, u órgano en el que éste delegue, previo informe del CNPIC, aprobará el Plan de Seguridad del Operador o las propuestas de mejora del mismo, notificando la resolución al interesado en el plazo máximo de dos meses.
2. Junto a la resolución de aprobación o modificación, el CNPIC, tomando en su caso como referencia las actuaciones del organismo regulador competente en virtud de la normativa sectorial aplicable, efectuará al operador crítico las recomendaciones que estime pertinentes, proponiendo en todo caso un calendario de implantación gradual donde se fije el orden de preferencia de las medidas y los procedimientos a adoptar.
3. El CNPIC gestionará y custodiará un registro central de todos los Planes de Seguridad del Operador existentes, una vez éstos sean aprobados por el Secretario de Estado de Seguridad. Los agentes del Sistema podrán tener acceso a los planes, previa comprobación por el CNPIC de su necesidad de conocer y con la autorización correspondiente.
4. Los Planes de Seguridad del Operador estarán clasificados conforme a lo que establece la legislación vigente en materia de secretos oficiales, debiendo constar expresamente en el instrumento de su aprobación. El CNPIC será responsable de garantizar a los agentes del Sistema autorizados el acceso a toda o parte de la información contenida en dichos planes velando por la confidencialidad y la seguridad de la misma. Por su parte, los operadores críticos responsables de la elaboración de los respectivos planes deberán custodiar los mismos implantando las medidas de seguridad de la información exigibles conforme a la Ley.

Artículo 24. *Revisión y actualización.*

1. Los Planes de Seguridad del Operador deberán ser revisados cada dos años por los operadores críticos y aprobados por el CNPIC. Éste podrá requerir en cualquier momento información concreta sobre el estado de implantación del Plan de Seguridad del Operador.

2. La modificación de alguno de los datos incluidos en los Planes de Seguridad del Operador obligará a la automática actualización de éstos, que se llevará a cabo por los operadores críticos responsables y requerirá la aprobación expresa del CNPIC.

CAPÍTULO IV

Los Planes de Protección Específicos

Artículo 25. *Finalidad, elaboración y contenido.*

1. Los Planes de Protección Específicos son los documentos operativos donde se deben definir las medidas concretas ya adoptadas y las que se vayan a adoptar por los operadores críticos para garantizar la seguridad integral (física y lógica) de sus infraestructuras críticas.

2. En el plazo de cuatro meses a partir de la aprobación del Plan de Seguridad del Operador, cada operador crítico deberá haber elaborado un Plan de Protección Específico por cada una de sus infraestructuras críticas así consideradas por la Secretaría de Estado de Seguridad y presentarlo al CNPIC. Igual procedimiento y plazos se establecerán cuando se identifique una nueva infraestructura crítica.

3. Los Planes de Protección Específicos de las diferentes infraestructuras críticas incluirán todas aquellas medidas que los respectivos operadores críticos consideren necesarias en función de los análisis de riesgos realizados respecto de las amenazas, en particular, las de origen terrorista, sobre sus activos, incluyendo los sistemas de información.

4. Cada Plan de Protección Específico deberá contemplar la adopción tanto de medidas permanentes de protección, sobre la base de lo dispuesto en el párrafo anterior, como de medidas de seguridad temporales y graduadas, que vendrán en su caso determinadas por la activación del Plan Nacional de Protección de las Infraestructuras Críticas, o bien como consecuencia de las comunicaciones que las autoridades competentes puedan efectuar al operador crítico en relación con una amenaza concreta sobre una o varias infraestructuras por él gestionadas.

5. La Secretaría de Estado de Seguridad, a través del CNPIC, establecerá los contenidos mínimos de los Planes de Protección Específicos, así como el modelo en el que fundamentar la estructura y la compleción de éstos que, en todo caso, cumplirán las directrices marcadas por sus respectivos Planes de Seguridad del Operador.

Artículo 26. *Aprobación, registro y clasificación.*

1. La Secretaría de Estado de Seguridad notificará al interesado, en el plazo máximo de dos meses contados a partir de la recepción, su resolución con la aprobación de los diferentes Planes de Protección Específicos o de las eventuales propuestas de mejora de éstos. Previamente, a través del CNPIC, se recabará informe preceptivo de las Delegaciones del Gobierno en las respectivas Comunidades Autónomas o en las Ciudades con Estatuto de Autonomía en el que se considerará, en su caso, el criterio de los órganos competentes de las Comunidades Autónomas con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público, así como del órgano u organismo competente para otorgar a los operadores críticos las autorizaciones correspondientes según la legislación sectorial vigente.

2. Junto a la resolución de aprobación o modificación, el CNPIC, basándose en los informes mencionados en el punto anterior, efectuará al operador crítico las recomendaciones que estime pertinentes, proponiendo en todo caso un calendario de implantación gradual donde se fije el orden de preferencia de las medidas y los procedimientos a adoptar sobre las infraestructuras afectadas.

3. Las Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía o, en su caso, el órgano competente de las Comunidades Autónomas con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público, mantendrán un registro donde obren, una vez sean aprobados por el Secretario de Estado de Seguridad, todos los Planes de Protección Específicos de las infraestructuras críticas o infraestructuras críticas europeas localizadas en su demarcación, y que deberán mantener permanentemente actualizado. En cualquier caso y sobre la base de lo anterior, el CNPIC gestionará y custodiará un registro

central de todos los Planes de Protección Específicos existentes. Los agentes del Sistema podrán tener acceso a los planes, previa comprobación por el CNPIC de su necesidad de conocer y con la autorización correspondiente.

4. Los Planes de Protección Específicos estarán clasificados conforme a lo que establece la legislación vigente en materia de secretos oficiales, debiendo constar expresamente en el instrumento de su aprobación. El CNPIC será responsable de garantizar a los agentes del Sistema autorizados el acceso a toda o a parte de la información contenida en dichos planes velando por la confidencialidad y la seguridad de la misma. Por su parte, los agentes del Sistema responsables de la elaboración de los respectivos planes y aquellos encargados de su registro deberán custodiar los mismos implantando las medidas de seguridad de la información exigibles conforme a la Ley.

Artículo 27. *Revisión y actualización.*

1. Los Planes de Protección Específicos deberán ser revisados cada dos años por los operadores críticos, revisión que deberá ser aprobada por las Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía o, en su caso, por el órgano competente de las Comunidades Autónomas con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público, y por el CNPIC.

2. La modificación de alguno de los datos incluidos en los Planes de Protección Específicos obligará a la automática actualización de éstos, que se llevará a cabo por los operadores críticos responsables y requerirá la aprobación expresa del CNPIC.

Artículo 28. *Aplicación y seguimiento.*

1. Los Delegados del Gobierno en las Comunidades Autónomas velarán por la correcta ejecución de los diferentes Planes de Protección Específicos y tendrán facultades de inspección en el ámbito de la protección de infraestructuras críticas. Dichas facultades deberán desarrollarse, en su caso, de forma coordinada con las facultades inspectoras del órgano u organismo competente para otorgar a los operadores críticos las autorizaciones correspondientes según la legislación sectorial vigente.

2. En aquellas Comunidades Autónomas con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público, las facultades de inspección serán ejercidas por sus órganos competentes, sin perjuicio de lo dispuesto en la legislación sectorial aplicable y de la necesaria coordinación con las Delegaciones del Gobierno en dichas Comunidades y los otros organismos reguladores competentes en virtud de su normativa sectorial.

3. En ejercicio de ese seguimiento, los organismos competentes podrán en todo momento requerir del responsable de las infraestructuras críticas o infraestructuras críticas europeas la situación actualizada de la implantación de las medidas propuestas en las resoluciones de aprobación o modificación de los Planes de Protección Específicos elaborados en caso de variación de las circunstancias que determinaron su adopción, o bien para adecuarlos a la normativa vigente que les afecte, dando cuenta del resultado de ello a la Secretaría de Estado de Seguridad, a través del CNPIC.

4. Las facultades de inspección en las instalaciones portuarias, así como en aquellos otros puntos o establecimientos considerados críticos que se encuentren integrados en un puerto, serán establecidas de acuerdo con lo previsto en el Real Decreto 1617/2007, de 7 de diciembre.

Artículo 29. *Compatibilidad con otros planes existentes.*

1. La elaboración de los Planes de Protección Específicos para cada una de las infraestructuras críticas se efectuará sin perjuicio del obligado cumplimiento de lo exigido por el Código Técnico de la Edificación, aprobado por el Real Decreto 314/2006, de 17 de marzo, el Real Decreto 393/2007, de 23 de marzo, por el que se aprueba la Norma Básica de Autoprotección de los centros, establecimientos y dependencias dedicados a actividades que puedan dar origen a situaciones de emergencia, la normativa de Seguridad Privada o cualquier otra reglamentación sectorial específica que le sea de aplicación.

2. Las instalaciones Nucleares e Instalaciones Radiactivas que se consideren críticas reguladas en el Reglamento sobre instalaciones nucleares y radiactivas, aprobado por el Real Decreto 1836/1999 de 3 de diciembre, modificado por el Real Decreto 35/2008 de 18 de enero, integrarán sus Planes de Protección Específicos en los respectivos Planes de Protección Física rigiéndose, en lo relativo a su aprobación y evaluación, por lo establecido en su normativa sectorial específica, sin perjuicio de lo que le sea de aplicación según la Ley 8/2011, de 28 de abril.

3. Las instalaciones portuarias, así como aquellos otros puntos o establecimientos considerados críticos que se encuentren integrados en un puerto, conforme a lo dispuesto en el Real Decreto 1617/2007, de 7 de diciembre, por el que se establecen medidas para la mejora de la protección de los puertos y el transporte marítimo, integrarán sus Planes de Protección Específicos en los Planes de Protección de Puertos previstos en el citado Real Decreto rigiéndose, en lo relativo a su aprobación y evaluación, por lo establecido en esa norma, sin perjuicio de lo que le sea de aplicación según la Ley 8/2011, de 28 de abril.

4. En el caso de aeropuertos, aeródromos e instalaciones de navegación aérea se considerarán Planes de Protección Específicos los respectivos Programas de Seguridad de los aeropuertos aprobados conforme a lo dispuesto en la Ley 21/2003, de 7 de julio, de Seguridad Aérea modificada por la Ley 1/2011, de 4 de marzo por la que se establece el Programa Estatal de Seguridad Operacional para la Aviación Civil y se modifica la Ley 21/2003, de 7 de julio de Seguridad Aérea y en el Real Decreto 550/2006, de 5 de mayo, por el que se designa la autoridad competente responsable de la coordinación y seguimiento del Programa Nacional de Seguridad para la Aviación Civil y se determina la organización y funciones del Comité Nacional de Seguridad de la Aviación Civil. No obstante, el Ministerio del Interior, a través de su representante en el Comité Nacional de Seguridad de la Aviación Civil podrá proponer contenidos adicionales, de conformidad con lo establecido en el artículo 25, apartado quinto de este real decreto.

CAPÍTULO V

Los Planes de Apoyo Operativo

Artículo 30. *Finalidad, elaboración y contenido.*

1. Los Planes de Apoyo Operativo son los documentos operativos donde se deben plasmar las medidas concretas a poner en marcha por las Administraciones Públicas en apoyo de los operadores críticos para la mejor protección de las infraestructuras críticas.

2. Por cada una de las infraestructuras críticas e infraestructuras críticas europeas dotadas de un Plan de Protección Específico y sobre la base a los datos contenidos en éste, la Delegación del Gobierno en la Comunidad Autónoma o, en su caso, el órgano competente de la Comunidad Autónoma, supervisará la realización de un Plan de Apoyo Operativo por parte del Cuerpo Policial estatal, o en su caso autonómico, con competencia en la demarcación territorial de que se trate. Para su elaboración, que deberá realizarse en un plazo de cuatro meses a partir de la aprobación del respectivo Plan de Protección Específico, se contará con la colaboración del responsable de seguridad de la infraestructura.

3. Sobre la base de sus correspondientes Planes de Protección Específicos, los Planes de Apoyo Operativo deberán contemplar, si las instalaciones lo precisan, las medidas planificadas de vigilancia, prevención, protección y reacción que deberán adoptar las unidades policiales y, en su caso, de las Fuerzas Armadas, cuando se produzca la activación del Plan Nacional de Protección de las Infraestructuras Críticas, o bien de confirmarse la existencia de una amenaza inminente sobre dichas infraestructuras. Estas medidas serán siempre complementarias a aquellas de carácter gradual que hayan sido previstas por los operadores críticos en sus respectivos Planes de Protección Específicos.

4. El CNPIC establecerá los contenidos mínimos de los Planes de Apoyo Operativo, así como el modelo en el que fundamentar la estructura y desarrollo de éstos, que se basarán en la parte que les corresponda en la información contenida en los respectivos Planes de Protección Específicos.

5. El Ministerio de Defensa podrá acceder a los Planes de Apoyo Operativo de aquellas infraestructuras críticas o infraestructuras críticas europeas que, en caso de activarse el Plan Nacional de Protección de las Infraestructuras Críticas y a los efectos de coordinar los correspondientes apoyos de las Fuerzas Armadas, se considere oportuno, previo estudio conjunto de los mencionados apoyos.

Artículo 31. *Aprobación, registro y clasificación.*

1. Los Planes de Apoyo Operativo serán validados y aprobados por la Secretaría de Estado de Seguridad, a través del CNPIC.

2. Las Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía o, en su caso, el órgano competente de cada Comunidad Autónoma con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público, mantendrán un registro donde obren, una vez sean validados, todos los Planes de Apoyo Operativo de las infraestructuras críticas e infraestructuras críticas europeas localizadas en su demarcación, y que deberán mantener permanentemente actualizado. En cualquier caso y sobre la base de lo anterior, el CNPIC gestionará y custodiará un registro central de todos los Planes de Apoyo Operativo existentes. Los agentes del Sistema podrán tener acceso a los planes, previa comprobación por el CNPIC de su necesidad de conocer y con la autorización correspondiente.

3. Los Planes de Apoyo Operativo estarán clasificados conforme a lo que establece la legislación vigente en materia de secretos oficiales, debiendo constar expresamente en el instrumento de su aprobación. El CNPIC será responsable de garantizar a los agentes del Sistema autorizados el acceso a toda o a parte de la información contenida en dichos planes velando por la confidencialidad y la seguridad de la misma. Por su parte, los agentes del Sistema responsables de la elaboración y registro de los respectivos planes deberán custodiar los mismos implantando las medidas de seguridad de la información exigibles conforme a la Ley.

Artículo 32. *Revisión y actualización.*

1. Los Planes de Apoyo Operativo deberán ser revisados cada dos años por el Cuerpo Policial estatal, o en su caso autonómico, con competencia en la demarcación territorial de que se trate, revisión que deberá ser aprobada por las Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía o, en su caso, por el órgano competente de las Comunidades Autónomas con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público, requiriendo la aprobación expresa del CNPIC.

2. La modificación de alguno de los datos incluidos en los Planes de Apoyo Operativo obligará a la automática actualización de éstos, que se llevará a cabo mediante el procedimiento previsto en el apartado primero.

TÍTULO IV

Comunicaciones entre los operadores críticos y las Administraciones públicas

Artículo 33. *Seguridad de las comunicaciones.*

1. El CNPIC será el responsable de administrar los sistemas de gestión de la información y comunicaciones que se diseñen en el ámbito de la protección de las infraestructuras críticas, que deberá contar para ello con el apoyo y colaboración de los agentes del Sistema y de todos aquellos otros organismos o entidades afectados.

2. La seguridad de los sistemas de información y comunicaciones previstos en este real decreto será acreditada y, en su caso, certificada por el Centro Criptológico Nacional del Centro Nacional de Inteligencia, de acuerdo con las competencias establecidas en su normativa específica.

3. La Presidencia del Gobierno facilitará el uso de la Malla B, sistema soporte de comunicaciones estratégicas seguras del Sistema Nacional de Gestión de Crisis y de la Presidencia del Gobierno, a través del cual los agentes del Sistema autorizados podrán

acceder a la información disponible en el Catálogo, con los niveles de acceso que se determinen.

Artículo 34. *El Responsable de Seguridad y Enlace.*

1. En el plazo de tres meses desde su designación como operadores críticos, los mismos nombrarán y comunicarán a la Secretaría de Estado de Seguridad, a través del CNPIC, el nombre del Responsable de seguridad y enlace en los términos y con los requisitos previstos por el artículo 16 de la Ley 8/2011, de 28 de abril.

2. El Responsable de Seguridad y Enlace representará al operador crítico ante la Secretaría de Estado de Seguridad en todas las materias relativas a la seguridad de sus infraestructuras y los diferentes planes especificados en este reglamento, canalizando, en su caso, las necesidades operativas e informativas que surjan al respecto.

Artículo 35. *El Delegado de Seguridad de la infraestructura crítica.*

1. En el plazo de tres meses desde la identificación como crítica o crítica europea, de una de sus infraestructuras, los operadores críticos comunicarán a las Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía o, en su caso, al órgano competente de la Comunidad Autónoma con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público donde aquéllas se ubiquen, la existencia e identidad de un Delegado de Seguridad para dicha infraestructura.

2. El Delegado de Seguridad constituirá el enlace operativo y el canal de información con las autoridades competentes en todo lo referente a la seguridad concreta de la infraestructura crítica o infraestructura crítica europea de que se trate, encauzando las necesidades operativas e informativas que se refieran a aquélla.

Artículo 36. *Seguridad de los datos clasificados.*

Los datos clasificados relativos a las infraestructuras de los operadores críticos cumplirán, en todo caso, con los requerimientos de seguridad establecidos por el Secretario de Estado Director del Centro Nacional de Inteligencia, de acuerdo con la normativa específica aplicable.

§ 24

Resolución de 8 de septiembre de 2015, de la Secretaría de Estado de Seguridad, por la que se aprueban los nuevos contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos

Ministerio del Interior
«BOE» núm. 224, de 18 de septiembre de 2015
Última modificación: sin modificaciones
Referencia: BOE-A-2015-10060

El Reglamento de protección de infraestructuras críticas aprobado por el Real Decreto 704/2011, de 20 de mayo, por el que se desarrolla la Ley 8/2011, de 28 de abril, en la que se establecen medidas para la protección de las infraestructuras críticas, dispone en los artículos 22.4 y 25.5 que la Secretaría de Estado de Seguridad establecerá, respectivamente, los contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos comprendidos en el artículo 14 de la Ley.

Dichos contenidos mínimos fueron recogidos en la Resolución de la Secretaría de Estado de Seguridad, de 15 de noviembre de 2011, resolución a su vez modificada por otra, de 29 de noviembre de 2011, que advertía y corregía determinados errores en la primera.

La constante evolución de la amenaza, la implantación de nuevas regulaciones, estrategias y herramientas de planificación, así como la experiencia adquirida en los últimos cuatro años, en buena parte, merced a las aportaciones efectuadas por los propios operadores críticos, hacen aconsejable la actualización de tales contenidos mínimos, con el fin de adecuar el nivel de planificación y respuesta a las exigencias requeridas para una eficaz protección de las infraestructuras críticas nacionales.

En virtud de ello, y conforme a lo preceptuado en el artículo 7, apartado e), del Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de Protección de las Infraestructuras Críticas, resuelvo aprobar y ordenar la publicación en el «Boletín Oficial del Estado» de los nuevos contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos que se insertan como anexo I y anexo II, respectivamente, de esta resolución.

La presente resolución deroga la precedente en esta misma materia, de la Secretaría de Estado de Seguridad, de 15 de noviembre de 2011, por la que se establecían los contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos, así como también la de 29 de noviembre de 2011, que modificaba la anterior.

ANEXO I

Guía Contenidos Mínimos

Plan de Seguridad del Operador (PSO)

Índice

1. Introducción.

1.1 Base Legal.
1.2 Objetivo de este Documento.
1.3 Finalidad y Contenido del PSO.
1.4 Método de Revisión y Actualización.
1.5 Protección y Gestión de la Información y Documentación.

2. Política General de Seguridad del Operador y Marco de Gobierno.

2.1 Política General de Seguridad del Operador Crítico.
2.2 Marco de Gobierno de Seguridad.

2.2.1 Organización de la Seguridad y Comunicación.
2.2.2 Formación y Concienciación.
2.2.3 Modelo de Gestión Aplicado.
2.2.4 Comunicación.

3. Relación de Servicios Esenciales prestados por el Operador Crítico.

3.1 Identificación de los Servicios Esenciales.
3.2 Mantenimiento del Inventario de Servicios Esenciales.
3.3 Estudio de las Consecuencias de la Interrupción del Servicio Esencial.
3.4 Interdependencias

4. Metodología de Análisis de Riesgos.

4.1 Descripción de la Metodología de Análisis.
4.2 Tipologías de Activos que Soportan los Servicios Esenciales.
4.3 Identificación y Evaluación de Amenazas.
4.4 Valoración y Gestión de Riesgos.

5. Criterios de aplicación de medidas de seguridad integral.
6. Documentación complementaria.

6.1 Normativa, Buenas Prácticas y Regulatoria.
6.2 Coordinación con Otros Planes.

1. Introducción.

1.1 Base legal.

El normal funcionamiento de los servicios esenciales que se prestan a la ciudadanía descansa sobre una serie de infraestructuras de gestión tanto pública como privada, cuyo funcionamiento es indispensable y no permite soluciones alternativas: las denominadas infraestructuras críticas. Por ello, se hace necesario el diseño de una política de seguridad homogénea e integral en el seno de las organizaciones que esté específicamente dirigida al ámbito de las infraestructuras críticas, en la cual se definan los subsistemas de seguridad que se van a implantar para la protección de las mismas con el objetivo de impedir su destrucción, interrupción o perturbación, con el consiguiente perjuicio de la prestación de los servicios esenciales a la población.

Este es precisamente el espíritu de la Ley 8/2011 de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, que tiene como objeto el establecer las estrategias y las estructuras organizativas adecuadas que permitan dirigir y coordinar las actuaciones de los distintos órganos de las administraciones públicas en materia de protección de infraestructuras críticas, previa identificación y designación de las mismas, impulsando la colaboración e implicación de los organismos y/o empresas gestoras

y propietarias (operadores críticos) de dichas infraestructuras, a fin de optimizar el grado de protección de éstas contra ataques deliberados tanto físicos como lógicos, que puedan afectar a la prestación de los servicios esenciales.

Dicha Ley tiene su desarrollo a través del Real Decreto 704/2011 de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

El artículo 13 de la Ley explicita una serie de compromisos para los operadores críticos públicos y privados, entre los que se encuentra la necesidad de elaboración de un Plan de Seguridad del operador (en adelante, PSO) y de los Planes de Protección Específicos que se determinen (en adelante, PPE).

Por su parte, el artículo 22.4 del Real Decreto 704/2011 responsabiliza a la Secretaría de Estado de Seguridad (órgano superior responsable del Sistema de Protección de Infraestructuras Críticas Nacionales, conforme al artículo 6 de la Ley 8/2011), a través del CNPIC, del establecimiento y puesta a disposición de los operadores críticos de los contenidos mínimos con los que deben contar los PSO, así como el modelo en el que basar la elaboración de los mismos.

1.2 Objetivo de este Documento.

Con el presente documento se pretende dar cumplimiento a las instrucciones emanadas del Real Decreto 704/2011, estableciendo los contenidos mínimos sobre los que se debe de apoyar un operador crítico a la hora del diseño y elaboración de su PSO. A su vez, se establecen algunos puntos explicativos sobre aspectos recogidos en la normativa de referencia.

Igualmente, se pretende orientar a aquellos operadores que hayan sido o vayan a ser designados como críticos en el diseño y elaboración de su respectivo Plan, con el fin de que estos puedan definir el contenido de su política general y el marco organizativo de seguridad, que encontrará su desarrollo específico en los PPE de cada una de sus infraestructuras críticas.

1.3 Finalidad y contenido del PSO.

El PSO definirá la política general del operador para garantizar la seguridad integral del conjunto de instalaciones o sistemas de su propiedad o gestión.

El PSO, como instrumento de planificación del Sistema de Protección de Infraestructuras Críticas, contendrá, además de un índice referenciado sobre los contenidos del Plan, información sobre:

- Política general de seguridad del operador y marco de gobierno.
- Relación de Servicios Esenciales prestados por el operador crítico.
- Metodología de análisis de riesgo (amenazas físicas y de ciberseguridad).
- Criterios de aplicación de Medidas de Seguridad Integral.

1.4 Método de revisión y actualización

Conforme al artículo 24 del Real Decreto 704/2011 de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas, entre las obligaciones del operador, además de la elaboración y presentación del PSO al Centro Nacional para la Protección de las Infraestructuras Críticas (en adelante CNPIC), se incluye su revisión y actualización periódica:

- Revisión: Bienal.
- Actualización: Cuando se produzca algún tipo de modificación en los datos incluidos en el PSO. En este caso, el PSO quedará actualizado cuando dichas modificaciones hayan sido validadas por el CNPIC, o en las condiciones establecidas en su normativa sectorial específica.

Independientemente de todo ello, en el caso de que varíen algunas de las circunstancias indicadas en el PSO (modificación de datos, identificación de nuevas infraestructuras críticas, baja de infraestructuras críticas, cese de condiciones para ser considerado operador crítico, etc…), el operador deberá trasladar la información oportuna al CNPIC, a través de los canales habilitados al efecto (Sistema HERMES/PoC oficial), en el plazo máximo de diez días a partir de las circunstancias variadas.

1.5 Protección y Gestión de la información y documentación.

La información es un valor estratégico para cualquier organización, siendo ésta de carácter sensible, por lo que en este sentido, el operador debe definir sus procedimientos de gestión y tratamiento, así como los estándares de seguridad precisos para prestar una adecuada y eficaz protección de esa información, independientemente del formato en el que ésta se encuentre.

Además, los operadores designados como críticos, deberán tratar los documentos que se deriven de la aplicación de la Ley 8/2011 y su desarrollo normativo a través del Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas, según el grado de clasificación que se derive de las citadas normas.

En virtud de la disposición adicional segunda de la ley 08/2011, la clasificación del PSO constará de forma expresa en el instrumento de su aprobación. A tal fin, el tratamiento de los PSO deberá estar regido conforme a las orientaciones publicadas por la Autoridad Nacional para la Protección de la Información Clasificada del Centro Nacional de Inteligencia en lo que se refiere al manejo y custodia de información clasificada con grado de Difusión Limitada.

Las orientaciones de referencia se encuentran recogidas en los siguientes documentos:

Seguridad documental.

OR-ASIP-04-01.04 – Orientaciones para el Manejo de Información Clasificada con Grado de Difusión Limitada.

Seguridad en el Personal.

OR-ASIP-04-02.02 – Instrucción de Seguridad del Personal para acceso a Información Clasificada.

Seguridad Física.

OR-ASIP-01-01.03 – Orientaciones para el Plan de Protección de una Zona de Acceso Restringido.

OR-ASIP-01-02.03–Orientaciones para la Constitución de Zonas de Acceso Restringido.

Seguridad de los Sistemas de Información y Comunicaciones.

OR-ASIP-03-01.04 – Orientaciones para la Acreditación de Sistemas de Información y Comunicaciones para el manejo de Información Clasificada.

2. Política General de Seguridad del Operador y Marco de seguridad.

2.1 Política General de Seguridad del Operador Crítico.

El objetivo de una Política de Seguridad es dirigir y dar soporte a la gestión de la seguridad. En ella, la Dirección de la Organización debe establecer claramente cuáles son sus líneas de actuación y manifestar su apoyo y compromiso con la seguridad.

Por tanto, en este apartado, el operador deberá reflejar el contenido de su Política de Seguridad de una forma homogénea e integral que esté específicamente dirigido al ámbito de las infraestructuras críticas y que sirva de marco de referencia para la protección de las mismas, con el objetivo de impedir su perturbación o destrucción.

Los aspectos mínimos que debe recoger la Política de Seguridad son:

• Objeto: La meta que pretende conseguir la Organización con la política y su posterior desarrollo y aplicación.

• Ámbito o Alcance de Aplicación: Una política puede estar limitada a determinados campos o aspectos o, por el contrario, ser de aplicación a toda la Organización. El operador deberá reflejar sobre qué partes de su Organización es aplicable la Política de Seguridad de protección de infraestructuras críticas, sin perder de vista que la misma ha de tener un carácter integral, considerando tanto la seguridad física como la ciberseguridad.

• Compromiso de la Alta Dirección: El operador debe garantizar que a la seguridad debe dársele la misma importancia que a otros factores de la producción o negocio de la organización.

Por ello, el compromiso de la Organización con la Política de Seguridad y lo que de ella se desarrolle deberá quedar plasmado mediante la aprobación, sanción y apoyo de la misma

por el órgano (Consejo de Administración, Consejo de Dirección, etc.) o la persona (Presidente, Consejero Delegado, etc.) de gobierno o dirección de la misma con capacidad suficiente para implantarla en la organización, así como su firme y explícito compromiso con la protección de los servicios esenciales prestados, compromiso que se debe ver reflejado en el propio plan.

• Carácter Integral de la Seguridad: La seguridad física y la ciberseguridad son áreas que deben ser abordadas de forma interrelacionada y con una perspectiva holística de la seguridad. Esto redundará en una visión global de la seguridad, posibilitando el diseño de una estrategia corporativa única, y optimizando el conocimiento, los recursos y los equipos. Por ello, el operador deberá remarcar el carácter integral de la seguridad aplicada a sus infraestructuras críticas, indicando en todo caso el procedimiento por el que se pretende alcanzar dicha seguridad integral: aspectos concretos de la organización, estructuras, procedimientos, etcétera. En este sentido, una respuesta integral a las diferentes amenazas existentes requiere la aplicación coordinada de medidas de seguridad física y ciberseguridad.

• Actualización de la Política General de Seguridad del Operador: Al ser la política de seguridad un documento de alto nivel, no suele requerir cambios significativos a lo largo del tiempo. No obstante, el operador deberá asegurarse de que ésta se mantenga actualizada y refleje aquellos cambios requeridos por variaciones en los activos a proteger, del entorno que les pueda afectar (amenazas, vulnerabilidades, impactos, salvaguardas), o en la reglamentación aplicable. En este apartado, el operador deberá recoger el proceso a seguir para la actualización y mantenimiento de su Política de Seguridad, incluyendo la periodicidad y el responsable de llevar a cabo estas acciones.

2.2 Marco de Gobierno de Seguridad.

2.2.1 Organización de la Seguridad y Comunicación.

El operador crítico debe designar a un Responsable de Seguridad y Enlace y a los Delegados de Seguridad en cada una de las infraestructuras críticas identificadas, así como a los sustitutos de ambos, de acuerdo a los requisitos establecidos en la Ley 8/2011. Deberá, por tanto, asegurar que se encuentren en un nivel jerárquico suficiente dentro de su estructura organizativa, de tal forma que los designados puedan garantizar el cumplimiento y la aplicación de la Política y de los requisitos establecidos para la protección de las infraestructuras críticas bajo su responsabilidad.

Asimismo, deberá asegurar la presencia física del delegado de seguridad en la infraestructura en un tiempo prudencial, en caso de que ello sea necesario.

En este apartado, el operador crítico deberá describir su organigrama de seguridad (comprendiendo tanto la Seguridad Física como la Ciberseguridad), con indicación de las figuras recogidas en la Ley, así como los niveles jerárquicos que les correspondan en su estructura organizativa.

Dicho organigrama debe incluir la ubicación física, estructura, jerarquía, órgano de gobierno e interrelación de todas las áreas de la organización con responsabilidad en cada uno de los ámbitos de la seguridad corporativa. Además, deberá dejar constancia de que los designados tienen capacidad suficiente para llevar a cabo todas aquellas acciones que se deriven de la aplicación de la Ley y el Real Decreto. En este sentido, el operador crítico deberá presentar:

• Un organigrama general, donde se identifique la estructura de seguridad corporativa.

• Un organigrama específico de la estructura de seguridad que integre la información sobre las distintas funciones que desempeña en la organización.

En su caso, el operador crítico deberá señalar los comités u órganos de decisión existentes en materia de seguridad, así como las funciones de cada uno de ellos.

Igualmente, se reflejarán los procedimientos de gestión y mantenimiento de la seguridad, haciendo constar si éstos son de carácter propio o son subcontratados. En este último caso, será necesario relacionar la empresa o empresas subcontratadas, las certificaciones en materia de seguridad con las que cuentan aquéllas, la sede desde la que se ejercen dichos servicios contratados, así como los servicios y compromisos acordados entre ambos. De igual forma, se definirá la metodología mediante la cual se lleva a cabo la comprobación del

cumplimiento por parte de la empresa contratada, con los protocolos de seguridad implementados en su caso por el operador.

En el campo de la ciberseguridad, y en lo relacionado con la protección de infraestructuras críticas, el CERT de Seguridad e Industria (en adelante CERTSI) es el responsable de la resolución de incidencias cibernéticas que puedan afectar a la prestación de los servicios esenciales gestionados por los

El CERTSI, en aplicación del Acuerdo Marco suscrito entre la Secretaría de Estado de Seguridad y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, da apoyo directo al CNPIC en todo lo relativo a la prevención y reacción ante incidentes que puedan afectar a las redes y sistemas de los operadores de infraestructuras críticas y a la disponibilidad de los servicios que éstos prestan.

Para todo ello, y previa suscripción de un acuerdo de confidencialidad entre las partes (operador crítico – CNPIC – CERTSI), dicho CERT podrá proporcionar servicios de prevención, detección, alerta temprana y respuesta a incidentes en apoyo a los departamentos encargados de esta labor en el seno de cada organización.

2.2.1.1 El Responsable de Seguridad y Enlace.

Conforme al artículo 16.2 de la Ley, el operador crítico deberá nombrar, en el plazo de tres meses desde su designación como tal, al Responsable de Seguridad y Enlace de la organización, que deberá estar habilitado por el Ministerio del Interior como Director de Seguridad, en virtud de lo dispuesto en el Real Decreto 2364/1994, de 9 de diciembre, en el que se aprueba el Reglamento de Seguridad Privada, o tener una habilitación equivalente, según su normativa sectorial específica. Tal nombramiento deberá ser comunicado a la Secretaría de Estado de Seguridad, a través del CNPIC.

El operador crítico deberá hacer constar en este apartado el nombre y datos de contacto (dirección, teléfonos y email) de la persona que fue designado como Responsable de Seguridad y Enlace así como de su sustituto, con idénticas condiciones, en ausencia del titular. Sus funciones en relación con el artículo 34.2 del Real Decreto 704/2011 son las siguientes:

• Representar al operador crítico ante la Secretaria de Estado de Seguridad:

– En materias relativas a la seguridad de sus infraestructuras.
– En lo relativo a los diferentes planes especificados en el Real Decreto.

• Canalizar las necesidades operativas e informativas que surjan entre el operador crítico y el CNPIC.

2.2.1.2 El Delegado de Seguridad de la Infraestructura Crítica.

Conforme al artículo 17 de la Ley, el operador crítico con infraestructuras designadas como críticas o críticas europeas comunicará a las Delegaciones del Gobierno o, en su caso, al órgano competente de la Comunidad Autónoma con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público donde aquéllas se ubiquen, la persona designada como Delegado de Seguridad y su sustituto. Esta comunicación deberá realizarse también al CNPIC, en el plazo de tres meses desde la notificación oficial de que es propietario o gestor de al menos una infraestructura crítica o crítica europea.

El operador crítico deberá hacer constar en este apartado el nombre y datos de contacto (dirección, teléfonos y email) de la persona designada como Delegado de Seguridad, así como de su sustituto, con idénticas condiciones, cumpliendo los plazos establecidos desde su designación como operador crítico, así como su participación a las Autoridades correspondientes, según lo establecido en el artículo 35.1 del Real Decreto 704/2011.

Es aconsejable que tanto el Delegado de Seguridad como su sustituto sean poseedores de titulación relativa a la rama de seguridad, además de pertenecer al departamento de seguridad de la entidad en cuestión.

Sus funciones en relación con el artículo 35.2 del Real Decreto 704/2011, son las siguientes:

• Ser el enlace operativo y el canal de información con las autoridades competentes en materias relativas a la seguridad de sus infraestructuras.

• Canalizar las necesidades operativas e informativas que surjan, a nivel infraestructura, entre el operador y las autoridades competentes.

2.2.2 Formación y Concienciación.

El operador crítico deberá colaborar con los programas o ejercicios que puedan derivarse del Plan Estratégico Sectorial, así como en su momento de los Planes de Apoyo Operativo.

El operador crítico reflejará en este apartado el Plan de Formación previsto para el personal relacionado con la protección de las infraestructuras críticas, indicando la duración, objetivos que se pretende conseguir, mecanismos de evaluación que se contemplan para el mismo y periodos de actualización. Así mismo, se incluirá el responsable del plan y la capacitación del mismo.

En el caso de que disponga de un Plan de Formación General, especificará la parte relacionada con la protección de las infraestructuras críticas, y la incluirá en este punto.

El operador crítico deberá reflejar en este apartado su participación en ejercicios de simulación en incidentes de seguridad (físicos y cibernéticos), y la periodicidad programada para tales ejercicios.

El personal implicado directamente en la protección de los servicios esenciales e infraestructuras críticas deberá ser formado para alcanzar conocimientos, a nivel básico:

• Sobre seguridad integral (seguridad física y ciberseguridad).
• Sobre autoprotección.
• Sobre seguridad del medio ambiente.
• Sobre habilidades organizativas y de comunicación.
• Sobre sus responsabilidades/actuaciones en caso de materializarse un incidente, o en el caso de que se active un nivel de amenaza 4 ó 5 del Plan de Prevención y Protección Antiterrorista y/o del Plan Nacional de Protección de las Infraestructuras Críticas.

El personal no directamente implicado deberá ser concienciado mediante la aplicación de las políticas de formación y operacionales activas en la organización.

2.2.3 Modelo de Gestión aplicado.

La seguridad integral depende de un proceso de gestión que debe aportar el control organizativo y técnico necesario para determinar en todo momento el nivel de exposición a las amenazas y el nivel de protección y respuesta que es capaz de proporcionar la organización para la protección y seguridad de sus servicios esenciales e Infraestructuras Críticas.

Por tanto, de acuerdo con la Política de Seguridad marcada, el operador crítico deberá recoger dentro del PSO su modelo de gestión elegido, que deberá contemplar como mínimo:

• Una implementación de controles de seguridad alineada con las prioridades y necesidades evaluadas.
• Una evaluación y monitorización continúa de la seguridad, con identificación de procesos y periodos.
• En el supuesto de que el operador crítico haya diseñado un sistema de gestión y/o la evaluación de la seguridad de las tecnologías de la información, de acuerdo a algún estándar de referencia internacional se debe indicar éste, así como las certificaciones que posee dicho sistema y el organismo certificador.

2.2.4 Comunicación.

El operador crítico deberá recoger explícitamente en este apartado los procedimientos establecidos para la comunicación e intercambio de información relativa a la protección de infraestructuras críticas, de la siguiente manera:

Comunicación al CNPIC:

• De aquellos incidentes o situaciones que puedan poner en riesgo o comprometer la seguridad de alguna de las infraestructuras de la que el operador es gestor y/o propietario, conforme al protocolo de comunicación de incidentes PIC elaborado por este Centro y puesto a disposición de los operadores críticos.

• De aquellas variaciones de carácter organizativo, de planificación o estructural que se produzcan en el seno del propio operador y que afecten de alguna manera a las infraestructuras críticas objeto de protección (por ejemplo, ajuste de cartera de servicios, fusiones, adquisiciones o ventas de activos, cambios técnicos, modificación de infraestructuras, cambio de instalaciones, etc.).

Comunicación al CERTSI:

• A través de la Oficina de Coordinación Cibernética del Ministerio del Interior (OCC), de los incidentes que puedan comprometer la seguridad cibernética de los sistemas y redes del operador crítico y la disponibilidad de los servicios que presta. Todo ello, conforme al protocolo de comunicación de incidentes PIC elaborado por el CNPIC y puesto a disposición de los operadores críticos.

3. Relación de Servicios esenciales prestados por el Operador Crítico.

El PSO deberá incluir, a modo de introducción, la información de contexto suficiente para describir los siguientes aspectos:

• Presentación general del operador crítico y sector/subsector principal/es de su actividad. En caso de grupos empresariales, se identificará claramente, con nombre y CIF, cuál de las empresas es el operador crítico.
• Estructura organizativa y societaria de todo el Grupo (en el caso de grupos empresariales).
• Presencia geográfica en los ámbitos nacional e internacional, con un resumen de las Comunidades Autónomas donde presten sus servicios esenciales, así como de aquellos países donde presten servicios similares.
• Principales líneas de actividad con la tipología general de servicios/productos que ofrecen.

3.1 Identificación de los Servicios esenciales.

El PSO deberá identificar aquellos servicios esenciales para la ciudadanía prestados por el operador a través del conjunto de sus infraestructuras estratégicas ubicadas en el territorio nacional, en relación al concepto de servicio esencial recogido en el artículo 2. a) de la Ley:

• Servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos.
• Eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas.

3.2 Mantenimiento del inventario de servicios esenciales.

Periódicamente, al menos bienalmente, el operador crítico deberá revisar la relación de servicios esenciales que figuran en su PSO, como consecuencia de la evolución normal que cualquier empresa experimenta respecto a los servicios que ofrece.
Así, en este mantenimiento deberá incorporar aquellos cambio/s que se produzcan:

• Por causas endógenas (por ejemplo, ajuste de cartera de servicios, fusiones, adquisiciones o ventas de activos, cambios técnicos, modificación de infraestructuras, cambio de instalaciones, etc.).
• Como consecuencia de la adecuación a los períodos establecidos en el Plan conforme al punto 1.4 de esta guía.

3.3 Estudio de las consecuencias de la interrupción del servicio esencial.

El operador crítico deberá llevar a cabo un estudio de las consecuencias que supondría la interrupción y no disponibilidad del servicio esencial que presta a la sociedad, motivado por:

• Alteración o interrupción temporal del servicio prestado.
• Destrucción parcial o total de la infraestructura que gestiona el servicio.
Adicionalmente, deberá identificar claramente, para cada uno de los casos anteriores, la siguiente información:

• Extensión geográfica y número de personas que pueden verse afectadas.

• Efecto sobre operadores y servicios esenciales dependientes.
• Existencia de alternativas de prestación del servicio esencial o mecanismos de contingencia proporcionados por el propio operador y nivel de degradación que conllevan.

3.4 Interdependencias.

En relación con el concepto de interdependencias recogido en el artículo 2. j) de la Ley, pueden existir efectos y repercusiones que afecten los servicios esenciales y las infraestructuras críticas propias y/o de otros operadores, tanto dentro del mismo sector como en otros sectores diferentes. Estas interdependencias deberán ser en todo caso consideradas en el análisis de riesgos que realicen los operadores en el marco global de su organización.

El operador crítico deberá hacer referencia a las interdependencias que identifique, explicando en líneas generales el motivo que origina dichas dependencias:

• Entre sus propias instalaciones o servicios.
• Con operadores del mismo sector.
• Con operadores de distintos sectores.
• Con operadores de otros países, del mismo sector o no.
• Con sus proveedores de servicio dentro de la cadena de suministros.
• Con los proveedores de servicios TIC contratados, tales como: proveedor(es) de telecomunicaciones, Centros de Proceso de Datos, servicios de seguridad (Centro de Operaciones de Seguridad, CERT privado, etcétera) y cualesquiera otros que se considere, especificando para cada uno de ellos el nombre del proveedor, los servicios contratados, acuerdos de nivel de servicio (SLA) y cumplimiento del servicio provisto con la política general de seguridad del operador.

4. Metodología del Análisis de Riesgos.

En virtud de lo establecido en el artículo 22.3 del Real Decreto 704/2011, en el PSO se plasmará la metodología o metodologías de análisis de riesgos empleadas por el operador crítico. Dichas metodologías deberán estar internacionalmente reconocidas, garantizar la continuidad de los servicios proporcionados por dicho operador y contemplar, de una manera global, tanto las amenazas físicas como lógicas existentes contra la totalidad de sus activos críticos. Todo ello, con independencia de las medidas mínimas que se puedan establecer para los Planes de Protección Específicos conforme a lo establecido por el artículo 25.

4.1 Descripción de la metodología de análisis.

Se describirá de forma genérica la metodología empleada por la Organización para la realización de los análisis de riesgos de los diferentes Planes de Protección Específicos (PPE) que se deriven tras la designación de sus infraestructuras críticas. Al menos, se aportará la siguiente información:

• Etapas esenciales.
• Algoritmos de cálculo empleados.
• Método empleado para la valoración de los impactos.
• Métricas de medición de riesgos aceptables, residuales, etc.
• En particular, se harán constar las relaciones entre los análisis de riesgos realizados a distintos niveles: A nivel de corporación, a nivel de servicios y el más concreto, a nivel de infraestructuras críticas.

4.2 Tipologías de activos que soportan los servicios esenciales.

Se denominan activos los recursos necesarios para que la Organización funcione correctamente y alcance los objetivos propuestos por su Dirección.

Sobre la base de los servicios identificados en el apartado 3.1 anterior, se incluirán en este apartado, para cada servicio esencial, los tipos de activos que los soportan, diferenciando aquéllos que son críticos de los que no lo son.

Las tipologías de activos a considerar serán, al menos:

• Las instalaciones necesarias para la prestación del servicio esencial.

• Los sistemas informáticos necesarios para dar soporte a los servicios esenciales (hardware y software).
• Las redes de comunicaciones necesarias para la prestación del servicio esencial.
• Las personas que explotan u operan todos los elementos anteriormente citados.

El objeto de esta sección es la identificación genérica de tipologías de activos asociadas a los servicios esenciales prestados por dicho operador, y sobre los que se focalizará el análisis de riesgos que efectúe el operador. El nivel de detalle será aquel que permita una comprensión del funcionamiento de los servicios, así como las interrelaciones entre activos y servicios.

Los activos no serán necesariamente espacios físicos concretos, pudiendo por ejemplo considerarse como activos sistemas distribuidos, tales como una red de datos.

4.3 Identificación y evaluación de amenazas.

En el marco de la normativa de protección de infraestructuras críticas y de cara a garantizar la adecuada protección de aquellas infraestructuras que prestan servicios esenciales, el operador crítico deberá tener como referencia el árbol de amenazas proporcionado por el CNPIC, considerando de forma especial aquellas amenazas de origen terrorista o intencionado. El operador deberá indicar expresamente las amenazas que ha considerado para la realización de los análisis de riesgos, plasmando al menos:

• Las intencionadas, de tipo tanto físico como lógico, que puedan afectar al conjunto de sus infraestructuras, las cuales deberán identificarse de forma específica en sus respectivos PPE, en su caso.
• Las procedentes de interdependencias, que puedan afectar directamente a los servicios esenciales, sean estas deliberadas o no.

4.4 Valoración y Gestión de Riesgos.

Los PSO recogerán la estrategia de gestión de riesgos implementada por el operador en cuanto a:

• Criterios utilizados para la valoración de las categorías de clasificación de los riesgos.
• Metodología de selección de estrategia (reducción, eliminación, transferencia, etc.).
• Plazos para la implantación de medidas, en el caso de elegir una estrategia de minimización del riesgo con indicación, si existe, de mecanismos de priorización de acciones.
• Tratamiento dado a las amenazas de ataques deliberados y, en particular, a aquellas que tengan una baja probabilidad pero un alto impacto debido a las consecuencias por su destrucción o interrupción en la continuidad de los servicios esenciales.
• Mecanismos de seguimiento y actualización periódicos de niveles de riesgo.

5. Criterios de aplicación de medidas de seguridad integral.

Dentro del ámbito de la seguridad integral, el operador definirá a grandes rasgos los criterios utilizados en su organización para la aplicación y administración de la seguridad. En este sentido, incluirá de forma genérica las medidas de seguridad implantadas en el conjunto de activos y recursos sobre los que se apoyan los servicios esenciales y que se recogerán en sus respectivos PPE, al objeto de hacer frente a las amenazas físicas y lógicas identificadas en los oportunos análisis de riesgos efectuados sobre cada una de las tipologías de sus activos.

6. Documentación complementaria.

6.1 Normativa, buenas prácticas y regulatoria.

El operador recogerá en una breve referencia motivada toda la normativa de aplicación y aquellas buenas prácticas que regulen el buen funcionamiento de los servicios esenciales prestados por todas y cada una de sus infraestructuras.

La normativa a incluir comprenderá la normativa general y sectorial, tanto de rango nacional, autonómico, europeo e internacional, relativas a:

• Seguridad Física.

• Ciberseguridad.
• Seguridad de la Información.
• Seguridad Personal.
• Seguridad Ambiental.
• Autoprotección y Prevención de Riesgos Laborales.

6.2 Coordinación con otros Planes.

Se identificarán todos aquellos Planes diseñados por el operador relativos a otros aspectos (continuidad de negocio, gestión del riesgo, respuesta, ciberseguridad, autoprotección, emergencias, etc.) que puedan coordinarse con el Plan de Seguridad del operador y los respectivos Planes de Protección Específicos que serán activados en el caso de que las medidas preventivas fallen y se produzca un incidente. Así mismo, debe dejarse constancia de la coordinación existente con el Plan Nacional para la Protección de las Infraestructuras Críticas.

ANEXO II

Guía de contenidos mínimos

Plan de Protección Específico (PPE)

Índice

1. Introducción.

1.1 Base Legal.
1.2 Objetivo de este Documento.
1.3 Finalidad y Contenido del PPE.
1.4 Método de Revisión y Actualización.
1.5 Protección y Gestión de la Información y Documentación.

2. Aspectos Organizativos.

2.1 Organigrama de Seguridad.
2.2 Delegados de Seguridad de las Infraestructuras Críticas.
2.3 Mecanismos de Coordinación.
2.4 Mecanismos y Responsables de Aprobación.

3. Descripción de la Infraestructura Crítica.

3.1 Datos Generales de la infraestructura crítica.
3.2 Activos/Elementos de la infraestructura crítica.
3.3 Interdependencias.

4. Resultados del Análisis de Riesgos.

4.1 Amenazas Consideradas.
4.2 Medidas de Seguridad Integral existentes.

4.2.1 Organizativas o de Gestión.
4.2.2 Operacionales o Procedimentales.
4.2.3 De Protección o Técnicas.

4.3 Valoración de Riesgos.

5. Plan de Acción propuesto (por activo).
6. Documentación complementaria.

1. Introducción.

1.1 Base legal.

Según establece la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, el operador designado como crítico, ya sea éste

perteneciente al sector público o al privado, se integrará como agente del sistema de protección de infraestructuras críticas, debiendo cumplir con una serie de responsabilidades recogidas en su artículo 13.

De acuerdo con en el punto 1, letra «d», del citado artículo, el operador deberá elaborar un Plan de Protección Específico (en adelante, PPE) por cada una de las infraestructuras críticas de las que sea propietario o gestor.

El Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas, a través del cual se da desarrollo reglamentario a la Ley 8/2011, establece, en su capítulo IV del Título III sobre los Instrumentos de Planificación, aquellos aspectos relativos a la elaboración, finalidad y contenido de dichos planes, además de su aprobación o modificación, registro, clasificación y formas de revisión y actualización, así como las autoridades encargadas de su aplicación y seguimiento, y la compatibilidad con otros planes ya existentes.

En este sentido, y conforme al artículo 25.5 de dicho real decreto, se asigna a la Secretaría de Estado de Seguridad, a través del Centro Nacional para la Protección de las Infraestructuras Críticas (en adelante, CNPIC), la responsabilidad de establecer los contenidos mínimos de los PPE, así como el modelo en el que fundamentar su estructura y compleción, sobre la base de las directrices y criterios marcados por el Plan de Seguridad del Operador (en adelante, PSO).

En el PPE, el operador crítico aplicará los siguientes aspectos y criterios incluidos en su PSO, que afecten de manera específica a esa instalación:

• Aspectos relativos a su política general de seguridad.

• Desarrollo de la metodología de análisis de riesgos que garantice la continuidad de los servicios proporcionados por dicho operador a través de esa infraestructura crítica.

• Desarrollo de los criterios de aplicación de las diferentes medidas de seguridad que se implanten para hacer frente a las amenazas, tanto físicas como aquellas que afectan a la ciberseguridad, identificadas en relación con cada una de las tipologías de los activos existentes en esa infraestructura.

1.2 Objetivo de este documento.

Con el presente documento se pretende dar cumplimiento a las instrucciones emanadas del Real Decreto 704/2011, estableciendo los contenidos mínimos sobre los que se debe apoyar el operador crítico a la hora de elaborar su respectivo PPE en las instalaciones catalogadas como críticas. A su vez, se establecen algunos puntos explicativos sobre aspectos recogidos en la Ley 8/2011 y el Real Decreto 704/2011.

1.3 Finalidad y contenido del PPE.

Los PPE son los documentos operativos donde se definen las medidas concretas a poner en marcha por los operadores críticos para garantizar la seguridad integral (seguridad física y ciberseguridad) de sus infraestructuras críticas.

Además de un índice referenciado a los contenidos del Plan, los PPE deberán contener, al menos, la siguiente información específica sobre la infraestructura a proteger:

• Organización de la seguridad.
• Descripción de la infraestructura.
• Resultado del análisis de riesgos:

Medidas de seguridad integral (tanto las existentes como las que sea necesario implementar) permanentes, temporales y graduales para las diferentes tipologías de activos a proteger y según los distintos niveles de amenaza declarados a nivel nacional de acuerdo con lo establecido por el Plan de Prevención y Protección Antiterrorista y por el Plan Nacional de Protección de Infraestructuras Críticas.

• Plan de acción propuesto (por cada activo evaluado en el análisis de riesgos).

Los PPE deberán estar alineados con las pautas establecidas en la Política General de Seguridad del operador reflejada en el PSO. Así mismo, los análisis de riesgos, vulnerabilidades y amenazas que se lleven a cabo, estarán sujetos a las pautas metodológicas descritas en el PSO.

1.4 Método de Revisión y Actualización.

Conforme al artículo 27 del Real Decreto por el que se aprueba el Reglamento de protección de las infraestructuras críticas, entre las obligaciones del operador crítico, además de la elaboración y presentación del PPE al CNPIC, se incluye su revisión y actualización periódica:

• Revisión: Bienal, que deberá ser aprobada por las Delegaciones del Gobierno en las CC.AA. y las Ciudades con Estatuto de Autonomía o, en su caso, por el órgano competente de las Comunidades Autónomas con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público, además de por parte del CNPIC.

• Actualización: Cuando se produzca una modificación en los datos incluidos dentro del PPE. En este caso, el PPE quedará actualizado cuando dichas modificaciones hayan sido validadas por el CNPIC, o en las condiciones establecidas en su normativa sectorial específica.

Independientemente de todo ello, en el caso de que varíen algunas de las circunstancias indicadas en el PPE (organización de la seguridad, datos de descripción de la infraestructura, medidas de seguridad, etc…), el operador deberá trasladar la información oportuna al CNPIC, a través de los canales habilitados al efecto (Sistema HERMES/PoC oficial), en el plazo máximo de diez días a partir de las circunstancias variadas.

1.5 Protección y Gestión de la Información y Documentación.

La información asociada con los PPE y aquélla relativa a los análisis de riesgos y las medidas de seguridad implantadas sobre las infraestructuras críticas a las que hacen referencia es de carácter sensible, por lo que, en este sentido, el operador deberá definir sus procedimientos de tratamiento de dicha información, así como los estándares de seguridad precisos para prestar una adecuada y eficaz protección de la información utilizados, independientemente del formato en el que ésta se encuentre.

Además, los operadores designados como críticos, deberán tratar los documentos que se deriven de la aplicación de la Ley 8/2011 y su desarrollo normativo a través del Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras, según el grado de clasificación que se derive de las citadas normas.

En virtud de la disposición adicional segunda de la Ley 08/2011, la clasificación del PPE constará de forma expresa en el instrumento de su aprobación. A tal fin, el tratamiento de los PPE deberá estar regido conforme a las orientaciones publicadas por la Autoridad Nacional para la Protección de la Información Clasificada del Centro Nacional de Inteligencia en lo que se refiere al manejo y custodia de información clasificada con grado de Difusión Limitada.

Las orientaciones de referencia se encuentran recogidas en los siguientes documentos:

Seguridad documental.

OR-ASIP-04-01.04.–Orientaciones para el Manejo de Información Clasificada con Grado de Difusión Limitada.

Seguridad en el personal.

OR-ASIP-04-02.02 – Instrucción de Seguridad del Personal para acceso a Información Clasificada.

Seguridad física.

OR-ASIP-01-01.03.–Orientaciones para el Plan de Protección de una Zona de Acceso Restringido.

OR-ASIP-01-02.03.–Orientaciones para la Constitución de Zonas de Acceso Restringido.

Seguridad de los Sistemas de Información y Comunicaciones.

OR-ASIP-03-01.04.–Orientaciones para la Acreditación de Sistemas de Información y Comunicaciones para el manejo de Información Clasificada.

2. Aspectos organizativos.

2.1 Organigrama de seguridad.

El operador crítico debe presentar gráficamente la estructura organizativa funcional que en materia de seguridad integral existe en la infraestructura crítica, con indicación de todos los actores que participan en aquella, su rol de responsabilidad y su jerarquía en el proceso de toma de decisiones. Del mismo modo, se debe establecer la dependencia de esta estructura con aquella definida en el correspondiente Plan de Seguridad del Operador.

2.2 Delegados de Seguridad de las Infraestructuras Críticas.

Conforme al artículo 17 de la Ley 8/2011, el operador crítico con infraestructuras designadas como críticas o criticas europeas comunicará a las Delegaciones del Gobierno en las CC.AA. y en las Ciudades con Estatuto de Autonomía o, en su caso, al órgano competente de la Comunidad Autónoma con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público donde aquellas se ubiquen, la persona designada como Delegado de Seguridad y su sustituto. Esta comunicación deberá realizarse también al CNPIC, en el plazo de tres meses desde la designación de una infraestructura como crítica.

El operador crítico deberá hacer constar en este apartado el nombre y datos de contacto (dirección, teléfonos y email) de la persona designada como Delegado de Seguridad así como de su sustituto, con idénticas condiciones, cumpliendo los plazos establecidos desde su designación, así como su participación a las Autoridades correspondientes, según lo establecido en el artículo 35.1 del Real Decreto 704/2011.

Es aconsejable que tanto el Delegado de Seguridad como su sustituto sean poseedores de titulación relativa a la rama de seguridad, además de pertenecer al departamento de seguridad de la entidad en cuestión.

Sus funciones en relación con el artículo 35.2 del Real Decreto 704/2011, son las siguientes:

• Ser el enlace operativo y el canal de información con las autoridades competentes en materia relativa a la seguridad de sus infraestructuras.
• Canalizar las necesidades operativas e informativas que surjan.

El operador crítico deberá reflejar en este apartado los cursos o formación que el Delegado de Seguridad haya recibido, relacionados con las habilidades necesarias para el desempeño del puesto, de acuerdo con el Plan de Formación previsto en el PSO.

2.3 Mecanismos de Coordinación.

El operador crítico deberá reflejar dentro de su PPE los mecanismos existentes de coordinación:

• Entre el Delegado de Seguridad de la infraestructura crítica con otros Delegados de otras infraestructuras críticas y con el Responsable de Seguridad y Enlace del propio operador.
• Con autoridades y terceros (Fuerzas y Cuerpos de Seguridad del Estado/Cuerpos Policiales autonómicos y locales/CNPIC/otros).
• Con otros planes existentes del operador (planes de continuidad de negocio, planes de evacuación, etc.).
• Con el CERT de Seguridad e Industria (CERTSI) identificando los puntos de contacto del operador en los 3 niveles requeridos: el institucional, y el directivo y el técnico, todos ellos referidos a en la gestión de incidentes.
• Con los proveedores críticos que se especifiquen a tenor del desarrollo de lo establecido en el punto 3.2.

2.4 Mecanismos y responsables de aprobación.

El operador deberá incluir dentro del PPE los siguientes aspectos relativos a su aprobación y revisión interna:

• Responsables de su aprobación.
• Procedimiento que se sigue para su aprobación.
• Fecha en la que se produjo su última aprobación.

• Responsable de su revisión y actualización.
• Aspectos objeto de revisión, en su caso.
• Registros generados por el procedimiento de revisión que permitan comprobar que el PPE ha sido revisado (reuniones, acta del Comité correspondiente, estudios y análisis realizados, actualizaciones de los análisis de riesgos, etc.).

3. Descripción de la Infraestructura Crítica.

3.1 Datos generales de la infraestructura crítica.

El operador crítico deberá incluir los siguientes datos e información sobre la infraestructura a proteger:

• Generales, relativos a la denominación y tipo de instalación, propiedad y gestión de la misma.
• Sobre localización física y estructura (localización, planos generales, fotografías, componentes, etc.)
• Sobre los sistemas TIC que gestionan la infraestructura crítica y su arquitectura.
• Datos estratégicos:

Descripción del servicio esencial que proporciona y el ámbito geográfico o poblacional del mismo.
Relación con otras posibles infraestructuras necesarias para la prestación de ese servicio esencial.
Descripción de sus funciones y de su relación con los servicios esenciales soportados.

3.2 Activos/elementos de la infraestructura críticas.

Se incluirán en este apartado todos los activos que soportan la infraestructura crítica, diferenciando aquellos que son vitales de los que no lo son. En concreto se detallarán:

• Las instalaciones o componentes de la infraestructura crítica que son necesarios y por lo tanto vitales para la prestación del servicio esencial.
• Los sistemas informáticos (hardware y software) utilizados, con especificación de los fabricantes, modelos y, versiones, etcétera.
• Las redes de comunicaciones que permiten intercambiar datos y que se utilicen para dicha infraestructura crítica:

Arquitectura de red, rangos de IP públicas y, dominios.
Esquema(s) de red completo y detallado, de tipo gráfico y con descripción literaria, donde se recojan los flujos de intercambio de información que se realizan en las redes, así como sus perímetros electrónicos.
Descripción de componentes de la red (servidores, terminales, hubs, switches, nodos, routers, firewalls,…) así como su ubicación física.

• Las personas o grupos de personas que explotan u operan todos los elementos anteriormente citados, indicando y detallando de forma particular si existe algún proceso externalizado a terceros.
• Los proveedores críticos que en general son necesarios para el funcionamiento de dicha infraestructura crítica, y específicamente:

De suministro eléctrico.
De comunicaciones (telefonía, internet, etc. …).
De tratamiento y almacenamiento de información (CPDs, etc.).
De ciberseguridad (CERTs privados, SOCs, etc.).

• Sobre los proveedores nombrados por el operador, se especificarán los distintos Acuerdos de Nivel de Servicios que se tienen contratados y que son considerados esenciales.

Del mismo modo, se especificarán las interdependencias existentes entre los diferentes activos que soportan o componen la infraestructura crítica. La información anterior deberá ser la suficiente para recoger de manera explícita el alcance de la infraestructura a proteger y con el mismo nivel de detalle que se haya establecido dentro del PSO.

3.3 Interdependencias.

En relación con el concepto de interdependencias recogido en el artículo 2. j) de la Ley, pueden existir efectos y repercusiones que afecten los servicios esenciales y las infraestructuras críticas propias y/o de otros operadores, tanto dentro del mismo sector como en ámbitos diferentes. Estas interdependencias deberán ser en todo caso consideradas en el análisis de riesgos que realicen los operadores para la infraestructura crítica de que se trate, en el marco del PPE.

El operador crítico deberá hacer referencia dentro de sus diferentes PPE a las interdependencias que, en su caso, identifique, explicando brevemente el motivo que las origina:

• Con otras infraestructuras críticas del propio operador.

• Con otras infraestructuras estratégicas del propio operador que soportan el servicio esencial.

• Entre sus propias instalaciones o servicios.

• Con sus proveedores dentro de la cadena de suministro.

• Con los proveedores de servicios TIC contratados para esa infraestructura, tales como: proveedor(es) de telecomunicaciones, Centros de Proceso de Datos, servicios de seguridad (Centro de Operaciones de Seguridad, CERT privado, etcétera) y cualesquiera otros que se considere, especificando para cada uno de ellos el nombre del proveedor, los servicios contratados, acuerdos de nivel de servicio (SLA) y cumplimiento del servicio provisto con la política general de seguridad del operador.

• Con los proveedores de servicios de seguridad física, indicando los servicios prestados y el personal y medios empleados.

4. Resultados del Análisis de Riesgos.

El operador crítico deberá reflejar en su PPE los resultados del análisis de riesgos integral realizado sobre la infraestructura crítica. Dicho análisis de riesgos deberá seguir las pautas metodológicas recogidas en su PSO.

A continuación se reflejan los contenidos mínimos relativos al análisis de riesgos realizado que el operador deberá incluir dentro del PPE.

4.1 Amenazas consideradas.

En el marco de la normativa de protección de infraestructuras críticas, y de cara a garantizar la adecuada protección de las infraestructuras críticas, el operador crítico deberá tener como referencia el árbol de amenazas proporcionado por el CNPIC, considerando de forma especial aquellas amenazas de origen terrorista o intencionado. El operador deberá indicar expresamente las amenazas que ha considerado para la realización de los análisis de riesgos, plasmando al menos:

• Las amenazas intencionadas, tanto de tipo físico como a la ciberseguridad, que afecten de forma específica a alguno de los activos que soportan la infraestructura crítica.

• Las amenazas que puedan afectar directamente a la infraestructura procedente de las interdependencias identificadas, sean éstas deliberadas o no.

• Las dirigidas al entorno cercano o elementos interdependientes tanto del ante-perímetro físico como lógico que puedan afectar a la infraestructura.

• Las amenazas que afecten a los sistemas de información que den soporte a la operación de la infraestructura crítica y todos los que estén conectados a dichos sistemas sin contar con las adecuadas medidas de segmentación.

• Las amenazas que afecten a los sistemas y servicios que soportan la seguridad integral.

4.2 Medidas de seguridad integral existentes.

El operador deberá describir las medidas de seguridad integral (medidas de protección de las instalaciones, equipos, datos, software de base y aplicativos, personal y documentación) implantadas en la actualidad, con las que se ha contado para la realización del análisis de riesgos. Deberá distinguir entre las medidas de carácter permanente, y aquellas temporales y graduales.

Por medidas permanentes se entienden aquellas medidas concretas ya adoptadas por el operador crítico, así como aquellas que considere necesarias instalar en función del resultado del análisis de riesgo realizado respecto de los riesgos, amenazas y consecuencias/impacto sobre sus activos, dirigidas todas ellas a garantizar la seguridad integral de su instalación catalogada como crítica de manera continua.

Por medidas temporales y graduales se entienden aquellas medidas de seguridad de carácter extraordinario que reforzarán a las permanentes y que se deberán implementar de forma ascendente a raíz de la activación de alguno de los niveles de seguridad establecidos respectivamente en el Plan Nacional de Protección de las Infraestructuras Críticas (artículo 16.3 del RD 704/2011), en coordinación con el Plan de Prevención y Protección Antiterrorista, principalmente para los niveles 4 y 5, o bien como consecuencia de las comunicaciones que las autoridades competentes puedan efectuar al operador crítico en relación con una amenaza concreta y temporal sobre la instalación por él gestionada.

Dichas medidas deberán permanecer activas durante el tiempo que esté establecido el nivel de alarma, modificándose gradualmente en función de dicho nivel.

Para su mejor comprensión, se recomienda una aproximación por capas para cada nivel, siendo la escala de niveles del 1 al 5 (nivel 1: riesgo bajo; nivel 2: riesgo moderado; nivel 3 riesgo medio; nivel 4: riesgo alto; nivel 5: riesgo muy alto), especificando para cada nivel las medidas de prevención y protección, el tiempo de respuesta y el tiempo de recuperación.

En concreto, el operador deberá describir las medidas concretas de que dispone relativas a:

4.2.1 Organizativas o de Gestión.

El operador deberá indicar si dispone de al menos de las siguientes medidas organizativas o de gestión, y el alcance de cada una de ellas:

• Análisis de Riesgos: Evaluación y valoración de las amenazas, impactos y probabilidades para obtener un nivel de riesgo.

• Definición de roles y responsabilidades: Asignación de responsabilidades en materia de seguridad.

• Cuerpo normativo definido: Políticas, procedimientos y estándares de seguridad.

• Normas y/o regulaciones de aplicación a la infraestructura crítica, así como identificación de su nivel de cumplimiento.

• Certificación, acreditación y evaluación de seguridad obtenidas para la infraestructura crítica.

4.2.2 Operacionales o Procedimentales.

El operador deberá indicar si dispone de al menos las siguientes medidas operacionales o procedimentales, y el alcance de cada una de ellas.

• Procedimientos para la realización, gestión y mantenimiento de activos críticos (ciclo de vida):

Identificación.
Adquisición.
Catalogación.
Alta.
Actualización.
Baja.

• Procedimientos de formación, concienciación y capacitación (tanto general como específica) para:

Empleados/Operarios.
Personal de seguridad.
Personal contratado.
Etc.

• Procedimientos de Contingencia/Recuperación, en función de los escenarios de contingencia que hayan sido definidos. Se deben detallar además los métodos y políticas de copias de respaldo (backup).

• Procedimientos operativos para la monitorización, supervisión y evaluación/auditoría de:

Activos Físicos de la infraestructura (Alcance/Operación/Seguimiento).
Activos Lógicos o de sistemas de operación (Alcance/Operación/Seguimiento).

• Procedimientos de seguridad.
• Procedimientos para la gestión de acceso:

Gestión de usuarios: Altas, bajas y modificaciones, procesos de selección, régimen interno, procedimientos de cese.
Control de accesos temporales:

De personas, vehículos, etc. al recinto general o a recintos restringidos.
Identificadores de usuario temporal de los sistemas (mantenimiento…).

Control de entradas y salidas:

Paquetería, correspondencia, etc.
Soportes, equipos e información (medidas y tecnologías de prevención de fuga de información).

• Procedimientos operacionales del personal de seguridad (funciones, horarios, dotaciones, etc.).
• Procedimientos de gestión y respuesta ante amenazas e incidentes.
• Procedimientos de comunicación e intercambio de información relativos a la protección de infraestructuras críticas (a través del protocolo de incidentes proporcionado por el CNPIC al efecto):

Con el CNPIC:

Sobre incidentes o situaciones que puedan poner en riesgo o comprometer la seguridad de la infraestructura.
Sobre variación de datos sobre la organización y medidas de seguridad, datos de descripción de la infraestructura, etc.

Con el CERTSI:

A través de la Oficina de Coordinación Cibernética del Ministerio del Interior (OCC), de los incidentes que puedan comprometer la seguridad cibernética de los sistemas y redes de la infraestructura y la disponibilidad de los servicios por ella prestada.

4.2.3 De Protección o Técnicas.

• Medidas de Prevención y Detección:

Medidas y elementos de seguridad física y electrónica para la protección del perímetro y control de accesos:

Vallas, zonas de seguridad, detectores de intrusos, cámaras de video vigilancia/CCTV, puertas y esclusas, cerraduras, lectores de matrículas, arcos de seguridad, tornos, scanners, tarjetas activas, lectores de tarjetas, etc.

Medidas y elementos de ciberseguridad:

• Firewalls, DMZ, IPSs, IDSs, segmentación y aislamiento de redes, cifrado, VPNs, elementos y medidas de control de acceso de usuarios (tokens, controles biométricos, etc.), medidas de instalación y configuración segura de elementos técnicos, correladores de eventos y logs, protección frente Malware, etc.
Redundancia de sistemas (hardware y software).

Otros.

• Medidas de Coordinación y Monitorización:

Centro de Control de Seguridad (control de alarmas, recepción y visionado de imágenes, etc.).
Equipos de vigilancia (turnos, rondas, volumen, etc.).

Sistemas de comunicación.
Otros.

4.3 Valoración de riesgos.

En este apartado se describirán las principales conclusiones obtenidas en el análisis de riesgos. Para cada par activo/amenaza se deberá especificar la valoración efectuada, sobre la base de los criterios especificados en la metodología de análisis de riesgos detallada en el PSO. Dentro de este apartado deberá incluirse, para cada par activo/amenaza, la siguiente información:

• Quién ha evaluado/aprobado el riesgo y la estrategia de tratamiento asociada.
• Criterios de valoración de riesgos adoptados.
• Fecha del último análisis llevado a cabo.
• Resultado/conclusión sobre el nivel de riesgo soportado.
• Evolución en el tiempo de la evaluación del par activo/amenaza

En particular, deberán detallarse los riesgos asumidos en activos con niveles de impacto elevado y baja probabilidad de ocurrencia, que deberán ser validados por el CNPIC.

5. Plan de acción propuesto (por activo).

En caso de ser pertinente y preverse la disposición de medidas complementarias a las existentes a implementar en los próximos tres años, se deberá describir, como parte integrante del PPE:

• Listado de las medidas complementarias a disponer (físicas o de ciberseguridad).
• Una explicación de la operativa resultante para cada tipo de protección (físico y lógico).

El operador deberá especificar el conjunto detallado de medidas a aplicar para proteger el activo como consecuencia de los resultados obtenidos en el análisis de riesgos. En concreto, deberá incluir la siguiente información:

• Activo de aplicación.
• Acción propuesta, con detalle de su ámbito (alcance) de aplicación.
• Responsables de su implantación, plazos, mecanismos de coordinación y seguimiento, etc.
• Carácter de la medida, permanente, temporal o gradual.

6. Documentación complementaria.

El operador crítico incorporará como anexo la planimetría general de la instalación o sistema y de sus sistemas de información, así como aquellos otros planos que incorporen la ubicación de las medidas de seguridad implementadas. A su vez, se podrá adjuntar aquella otra información que se pueda generar de los diferentes apartados de este documento.

Se hará una breve referencia a todos aquellos planes de diferente tipo (emergencia, autoprotección, ciberseguridad, etc.), que afecten a la instalación o sistema con el fin de establecer una adecuada coordinación entre ellos, así como toda aquella normativa y buenas prácticas que regulen el buen funcionamiento del servicio esencial prestado por esa infraestructura y los motivos por los cuales le son de aplicación.

La normativa a incluir comprenderá la normativa general y sectorial, tanto de rango nacional, autonómico, europeo e internacional, relativas a:

• Seguridad Física.
• Ciberseguridad.
• Seguridad de la Información.
• Seguridad Personal.
• Seguridad Ambiental.
• Autoprotección y Prevención de Riesgos Laborales.

§ 25

Orden INT/859/2023, de 21 de julio, por la que se desarrolla la estructura orgánica y funciones de los servicios centrales y territoriales de la Dirección General de la Policía. [Inclusión parcial]

Ministerio del Interior
«BOE» núm. 176, de 25 de julio de 2023
Última modificación: 17 de agosto de 2023
Referencia: BOE-A-2023-17072

[. . .]

CAPÍTULO II

Organización central

Sección 1.ª Dirección General de la Policía

[. . .]

Artículo 6. *Comisaría General de Policía Judicial.*

1. Asume las funciones contempladas en el artículo 3.3.b) del Real Decreto 734/2020, de 4 de agosto.

2. Está integrada por las siguientes Unidades:

a) La Unidad Central de Coordinación Operativa y Técnica. En su función de asistencia y apoyo a la persona titular de la Comisaría General, le corresponde generar el conocimiento para la realización y coordinación de la planificación operativa de ese Centro Directivo, facilitando las líneas generales de actuación para la configuración del Plan Estratégico en su área competencial. Coordina la actividad operativa y proporciona apoyo técnico a las unidades centrales y territoriales, asumiendo el seguimiento de la ejecución de las decisiones adoptadas. Gestiona los recursos humanos y los medios materiales adscritos al servicio, implementando las medidas necesarias para obtener un mayor nivel de eficiencia. Define los procedimientos de gestión. Promueve las actividades de I+D+i en colaboración con la Subdirección General competente. Asimismo, coordina la colaboración internacional de la Comisaría General.

La persona responsable de esta Unidad, denominada Jefa o Jefe Central de Operaciones, sustituye a la persona titular de la Comisaría General en los casos de vacante, ausencia o enfermedad.

De esta Unidad dependen:

1.º La Brigada de Coordinación Operativa. Le compete planificar y coordinar las operaciones de su ámbito funcional, ejerciendo la supervisión de los servicios en el nivel central.

2.º La Secretaría General. Le corresponde la gestión de los recursos humanos, la formación y los medios materiales adscritos a la Comisaría General, prestando asistencia técnica, jurídica y administrativa a las unidades centrales y territoriales que conforman el área funcional de policía judicial.

b) La Unidad Central de Droga y Crimen Organizado. Le corresponde la investigación y persecución de las actividades delictivas, de ámbito nacional e internacional, relacionadas con el tráfico de drogas y el crimen organizado, así como la coordinación operativa y el apoyo técnico de las respectivas unidades territoriales.

De esta Unidad dependen:

1.º La Brigada Central de Estupefacientes. Le compete la investigación y persecución de los delitos relacionados con el tráfico ilegal de drogas con arreglo a la legislación sobre la materia.

2.º La Brigada Central de Crimen Organizado. Se encarga de la investigación y persecución de las actividades delictivas vinculadas a la delincuencia organizada y la dirección de los Grupos de Respuesta contra el Crimen Organizado desplegados en diversas zonas del territorio español.

3.º La Unidad Adscrita a la Fiscalía General del Estado. Desempeña los cometidos que, como policía judicial, le asigne el órgano al que figura adscrita.

c) La Unidad Central de Delincuencia Especializada y Violenta. Le corresponde la investigación y persecución de las actividades delictivas, tanto de ámbito nacional como internacional, en lo concerniente a los delitos contra las personas y contra el patrimonio, especialmente el patrimonio histórico artístico, los relativos a los derechos de autor, consumo y medio ambiente, así como los cometidos en materia de dopaje y corrupción en el deporte. Se encarga de la vigilancia e inspección del juego, la coordinación operativa de las respectivas unidades territoriales y el apoyo técnico de las mismas. Además, se constituye como punto de contacto en todas las materias mencionadas, especialmente en asuntos relativos al patrimonio histórico, el juego y los desaparecidos, dependiendo funcionalmente de esta Unidad los delegados provinciales en las mencionadas materias.

De esta Unidad dependen:

1.º La Brigada Central de Investigación de la Delincuencia Especializada. Le compete la investigación y persecución de los delitos relacionados con el patrimonio, la propiedad intelectual e industrial y los específicamente cometidos contra el patrimonio histórico.

2.º La Brigada Central de Investigación de Delitos contra las Personas. Se encarga de la investigación y persecución de los delitos contra la vida, la libertad, los consumidores, el medio ambiente y el dopaje deportivo, así como de la investigación de las desapariciones de personas mayores de edad.

d) La Unidad Central de Inteligencia Criminal. Le corresponde la captación, recepción, tratamiento, coordinación, análisis, intercambio y desarrollo de las informaciones relativas a la delincuencia organizada y la criminalidad en general, como órgano de desarrollo de la función de inteligencia criminal y de apoyo para las funciones de dirección, planificación y toma de decisiones. Asume el impulso y ejecución del análisis de la criminalidad, como herramienta para la resolución de investigaciones complejas en el marco de la delincuencia organizada y grave. Lleva a cabo la actividad prospectiva en su ámbito competencial. Igualmente, se encarga de la elaboración, desarrollo y seguimiento de la planificación estratégica.

e) La Unidad Central de Delincuencia Económica y Fiscal. Le corresponde la investigación y persecución de las actividades delictivas, de ámbito nacional e internacional, en materia de delincuencia económica y fiscal, la coordinación operativa de las respectivas unidades territoriales, así como el apoyo técnico a las mismas.

De esta Unidad dependen:

1.º La Brigada Central de Delincuencia Económica y Fiscal. Le compete la investigación y persecución de los delitos contra las Haciendas Públicas, la Seguridad Social y sus Entidades Gestoras en sus distintas modalidades y contra los derechos de los trabajadores, los fraudes financieros, el espionaje industrial y las estafas de especial trascendencia.

2.º La Brigada Central de Investigación de Blanqueo de Capitales y Anticorrupción. Se encarga de la investigación y persecución de los hechos delictivos relacionados con el blanqueo de capitales, los delitos económicos relacionados con la piratería internacional, la corrupción en sus distintas modalidades y la localización y recuperación de activos.

3.º La Brigada Central de Inteligencia Financiera. Le corresponde la investigación y persecución de los delitos relacionados con las actividades y los sujetos regulados por la normativa de prevención del blanqueo de capitales.

4.º La Brigada de Investigación del Banco de España. Le compete la investigación y persecución de los delitos relacionados con la falsificación de moneda nacional y extranjera, constituyéndose como Oficina Central Nacional en este ámbito.

5.º La Unidad Adscrita a la Fiscalía Especial contra la Corrupción y la Criminalidad Organizada. Desempeña los cometidos que, como policía judicial, le asigne el órgano al que figura adscrita.

f) La Unidad Central de Ciberdelincuencia. Le corresponde la investigación y persecución, a nivel nacional e internacional, de las actividades delictivas en las que el uso de las nuevas tecnologías o sistemas de información supongan el instrumento o medio fundamental de comisión y que estén relacionadas con el patrimonio, el consumo, la indemnidad del menor, la pornografía infantil, la libertad sexual, el honor, la intimidad, las redes sociales, los fraudes, la propiedad intelectual e industrial; así como de aquellas que atenten contra la confidencialidad, la integridad y la disponibilidad de los sistemas de información y comunicaciones. Se constituye como Centro de Prevención y Respuesta E-Crime de la Policía Nacional.

De esta Unidad dependen:

1.º La Brigada Central de Investigación Tecnológica. Le compete la investigación de los delitos contra las personas cometidos mediante el uso de las nuevas tecnologías, como es el caso de los relacionados con la explotación sexual infantil en sus diferentes modalidades y todos aquellos llevados a cabo mediante el uso de las redes sociales y las páginas web, facilitando la coordinación y el apoyo al resto de unidades.

2.º La Brigada Central de Seguridad Informática. Se encarga de la persecución de delitos de alta especialización relacionados con ciberataques, creación y distribución de software malicioso, utilización de criptovalores como mecanismo de intercambio monetario en el entorno cibercriminal, delitos contra la propiedad intelectual cometidos mediante la utilización de las nuevas tecnologías y fraudes BEC (Business Email Compromise), así como del apoyo a las unidades de esta Comisaría General y unidades territoriales. Asimismo, se constituye como punto de contacto del Convenio de Budapest.

3.º La Brigada Central de Fraudes Informáticos. Le corresponde la investigación de todas las tipologías delictivas relacionadas con los fraudes cometidos a través de internet y el uso de las telecomunicaciones, incluyendo el ámbito electrónico, los diferentes medios de pago y el fraude bancario y empresarial cuando el uso de las nuevas tecnologías o de sistemas de información supongan el instrumento o medio fundamental para la comisión de las conductas delictivas.

g) La Unidad Central de Atención a la Familia y Mujer. Le corresponde la investigación y persecución de las infracciones penales en el ámbito de la violencia de género y doméstica, así como de la sexual, con independencia de la relación entre la víctima y autor. Coordina la actividad de protección de las víctimas de la especialidad. Igualmente, es el referente policial en materia de menores.

De esta Unidad dependen:

1.º La Brigada Operativa de Atención a la Familia y Mujer. Le compete la coordinación de la actuación de la función de investigación y persecución de los delitos de la especialidad y la protección de sus víctimas.

2.º La Oficina de Estudios. Se encarga del seguimiento y análisis de los delitos conocidos en este ámbito, promoviendo iniciativas y medidas dirigidas a la lucha contra el problema social que estas violencias suponen, y la coordinación con otros organismos nacionales e internacionales con competencia en estas materias.

h) El Gabinete. Dependiendo directamente de la persona titular de la Comisaría General, con funciones de asistencia inmediata y el apoyo en el desarrollo de sus funciones directivas.

[. . .]

§ 26

Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana

Jefatura del Estado
«BOE» núm. 77, de 31 de marzo de 2015
Última modificación: 23 de febrero de 2021
Referencia: BOE-A-2015-3442

FELIPE VI

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley orgánica:

PREÁMBULO

I

La seguridad ciudadana es la garantía de que los derechos y libertades reconocidos y amparados por las constituciones democráticas puedan ser ejercidos libremente por la ciudadanía y no meras declaraciones formales carentes de eficacia jurídica. En este sentido, la seguridad ciudadana se configura como uno de los elementos esenciales del Estado de Derecho.

Las demandas sociales de seguridad ciudadana van dirigidas esencialmente al Estado, pues es apreciable una conciencia social de que sólo éste puede asegurar un ámbito de convivencia en el que sea posible el ejercicio de los derechos y libertades, mediante la eliminación de la violencia y la remoción de los obstáculos que se opongan a la plenitud de aquellos.

La Constitución Española de 1978 asumió el concepto de seguridad ciudadana (artículo 104.1), así como el de seguridad pública (artículo 149.1.29.ª). Posteriormente, la doctrina y la jurisprudencia han venido interpretando, con matices, estos dos conceptos como sinónimos, entendiendo por tales la actividad dirigida a la protección de personas y bienes y al mantenimiento de la tranquilidad ciudadana.

Es a la luz de estas consideraciones como se deben interpretar la idea de seguridad ciudadana y los conceptos afines a la misma, huyendo de definiciones genéricas que justifiquen una intervención expansiva sobre los ciudadanos en virtud de peligros indefinidos, y evitando una discrecionalidad administrativa y una potestad sancionadora genéricas.

Para garantizar la seguridad ciudadana, que es una de las prioridades de la acción de los poderes públicos, el modelo de Estado de Derecho instaurado por la Constitución dispone de tres mecanismos: un ordenamiento jurídico adecuado para dar respuesta a los

diversos fenómenos ilícitos, un Poder Judicial que asegure su aplicación, y unas Fuerzas y Cuerpos de Seguridad eficaces en la prevención y persecución de las infracciones.

En el marco del artículo 149.1.29.ª de la Constitución y siguiendo las orientaciones de la doctrina constitucional, esta Ley tiene por objeto la protección de personas y bienes y el mantenimiento de la tranquilidad ciudadana, e incluye un conjunto plural y diversificado de actuaciones, de distinta naturaleza y contenido, orientadas a una misma finalidad tuitiva del bien jurídico protegido. Una parte significativa de su contenido se refiere a la regulación de las intervenciones de la policía de seguridad, funciones propias de las Fuerzas y Cuerpos de Seguridad, aunque con ello no se agota el ámbito material de lo que hay que entender por seguridad pública, en el que se incluyen otras materias, entre las que la Ley aborda las obligaciones de registro documental o de adopción de medidas de seguridad por las personas físicas o jurídicas que realicen actividades relevantes para la seguridad ciudadana, o el control administrativo sobre armas y explosivos, entre otras.

II

La Ley Orgánica 1/1992, de 21 de febrero, sobre Protección de la Seguridad Ciudadana, constituyó el primer esfuerzo por abordar, desde la óptica de los derechos y valores constitucionales, un código que recogiera las principales actuaciones y potestades de los poderes públicos, especialmente de las Fuerzas y Cuerpos de Seguridad, a fin de garantizar la seguridad de los ciudadanos.

Sin embargo, varios factores aconsejan acometer su sustitución por un nuevo texto. La perspectiva que el transcurso del tiempo ofrece de las virtudes y carencias de las normas jurídicas, los cambios sociales operados en nuestro país, las nuevas formas de poner en riesgo la seguridad y la tranquilidad ciudadanas, los nuevos contenidos que las demandas sociales incluyen en este concepto, la imperiosa necesidad de actualización del régimen sancionador o la conveniencia de incorporar la jurisprudencia constitucional en esta materia justifican sobradamente un cambio legislativo.

Libertad y seguridad constituyen un binomio clave para el buen funcionamiento de una sociedad democrática avanzada, siendo la seguridad un instrumento al servicio de la garantía de derechos y libertades y no un fin en sí mismo.

Por tanto cualquier incidencia o limitación en el ejercicio de las libertades ciudadanas por razones de seguridad debe ampararse en el principio de legalidad y en el de proporcionalidad en una triple dimensión: un juicio de idoneidad de la limitación (para la consecución del objetivo propuesto), un juicio de necesidad de la misma (entendido como inexistencia de otra medida menos intensa para la consecución del mismo fin) y un juicio de proporcionalidad en sentido estricto de dicha limitación (por derivarse de ella un beneficio para el interés público que justifica un cierto sacrificio del ejercicio del derecho).

Son estas consideraciones las que han inspirado la redacción de esta Ley, en un intento de hacer compatibles los derechos y libertades de los ciudadanos con la injerencia estrictamente indispensable en los mismos para garantizar su seguridad, sin la cual su disfrute no sería ni real ni efectivo.

III

La Ley, de acuerdo con la jurisprudencia constitucional, parte de un concepto material de seguridad ciudadana entendida como actividad dirigida a la protección de personas y bienes y al mantenimiento de la tranquilidad de los ciudadanos, que engloba un conjunto plural y diversificado de actuaciones, distintas por su naturaleza y contenido, orientadas a una misma finalidad tuitiva del bien jurídico así definido. Dentro de este conjunto de actuaciones se sitúan las específicas de las organizaciones instrumentales destinadas a este fin, en especial, las que corresponden a las Fuerzas y Cuerpos de Seguridad, a las que el artículo 104 de la Constitución encomienda proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana. Junto a esas actividades policiales en sentido estricto, la Ley regula aspectos y funciones atribuidos a otros órganos y autoridades administrativas, como la documentación e identificación de las personas, el control administrativo de armas, explosivos, cartuchería y artículos pirotécnicos o la previsión de la necesidad de adoptar medidas de seguridad en determinados establecimientos, con el correlato de un régimen

sancionador actualizado imprescindible para garantizar el cumplimiento de los fines de la Ley.

La Ley se estructura en cinco capítulos divididos en cincuenta y cuatro artículos, siete disposiciones adicionales, una transitoria, una derogatoria y cinco finales.

El capítulo I, tras definir el objeto de la Ley, recoge como novedades más relevantes sus fines y los principios rectores de la actuación de los poderes públicos en el ámbito de la seguridad ciudadana, la cooperación interadministrativa y el deber de colaboración de las autoridades y los empleados públicos, los distintos cuerpos policiales, los ciudadanos y las empresas y el personal de seguridad privada, de acuerdo con una perspectiva integral de la seguridad pública. Entre los fines de la Ley destacan la protección del libre ejercicio de los derechos fundamentales y las libertades públicas y los demás derechos reconocidos y amparados por el ordenamiento jurídico; la garantía del normal funcionamiento de las instituciones; la preservación no sólo de la seguridad, sino también de la tranquilidad y la pacífica convivencia ciudadanas; el respeto a las Leyes en el ejercicio de los derechos y libertades; la protección de las personas y bienes, con especial atención a los menores y a las personas con discapacidad necesitadas de especial protección; la pacífica utilización de vías y demás bienes demaniales destinados al uso y disfrute público; la garantía de la normal prestación de los servicios básicos para la comunidad; y la transparencia en la actuación de los poderes públicos en materia de seguridad ciudadana.

El capítulo II regula la documentación e identificación de los ciudadanos españoles, el valor probatorio del Documento Nacional de Identidad y del pasaporte y los deberes de los titulares de estos documentos, incorporando las posibilidades de identificación y de firma electrónica de los mismos, y manteniendo la exigencia de exhibirlos a requerimiento de los agentes de la autoridad de conformidad con lo dispuesto en la Ley.

El capítulo III habilita a las autoridades competentes para acordar distintas actuaciones dirigidas al mantenimiento y, en su caso, al restablecimiento de la tranquilidad ciudadana en supuestos de inseguridad pública, regulando con precisión los presupuestos, los fines y los requisitos para realizar estas diligencias, de acuerdo con los principios, entre otros, de proporcionalidad, injerencia mínima y no discriminación.

En este sentido, se regulan con detalle las facultades de las autoridades y de los agentes de las Fuerzas y Cuerpos de Seguridad para dictar órdenes e instrucciones, para la entrada y registro en domicilios, requerir la identificación de personas, efectuar comprobaciones y registros en lugares públicos, establecer restricciones del tránsito y controles en la vía pública, así como otras medidas extraordinarias en situaciones de emergencia imprescindible para garantizar la seguridad ciudadana (desalojo de locales o establecimientos, prohibición de paso, evacuación de inmuebles, etc.). Igualmente se regulan las medidas que deberán adoptar las autoridades para proteger la celebración de reuniones y manifestaciones, así como para restablecer la normalidad de su desarrollo en casos de alteración de la seguridad ciudadana.

La relación de estas potestades de policía de seguridad es análoga a la contenida en la Ley Orgánica 1/1992, de 21 de febrero, si bien, en garantía de los derechos de los ciudadanos que puedan verse afectados por su legítimo ejercicio por parte de los miembros de las Fuerzas y Cuerpos de Seguridad, se perfilan con mayor precisión los presupuestos habilitantes y las condiciones y requisitos de su ejercicio, de acuerdo con la jurisprudencia constitucional. Así, la habilitación a los agentes de las Fuerzas y Cuerpos de Seguridad para la práctica de identificaciones en la vía pública no se justifica genéricamente –como sucede en la Ley de 1992– en el ejercicio de las funciones de protección de la seguridad ciudadana, sino que es precisa la existencia de indicios de participación en la comisión de una infracción, o que razonablemente se considere necesario realizar la identificación para prevenir la comisión de un delito; por otra parte, en la práctica de esta diligencia, los agentes deberán respetar escrupulosamente los principios de proporcionalidad, igualdad de trato y no discriminación, y sólo en caso de negativa a la identificación, o si ésta no pudiera realizarse in situ, podrá requerirse a la persona para que acompañe a los agentes a las dependencias policiales más próximas en las que pueda efectuarse dicha identificación, informándola de modo inmediato y comprensible de los fines de la solicitud de identificación y, en su caso, de las razones del requerimiento.

Por primera vez se regulan los registros corporales externos, que sólo podrán realizarse cuando existan motivos para suponer que pueden conducir al hallazgo de instrumentos, efectos u otros objetos relevantes para el ejercicio de las funciones de indagación y prevención que encomiendan las Leyes a las Fuerzas y Cuerpos de Seguridad. Estos registros, de carácter superficial, deberán ocasionar el menor perjuicio a la dignidad de la persona, efectuarse por un agente del mismo sexo que la persona sobre la que se practique y, cuando lo exija el respeto a la intimidad, en un lugar reservado y fuera de la vista de terceros.

El capítulo IV, referente a las potestades especiales de la policía administrativa de seguridad, regula las medidas de control administrativo que el Estado puede ejercer sobre las actividades relacionadas con armas, explosivos, cartuchería y artículos pirotécnicos.

Asimismo, se establecen obligaciones de registro documental para actividades relevantes para la seguridad ciudadana, como el hospedaje, el acceso comercial a servicios telefónicos o telemáticos de uso público mediante establecimientos abiertos al público, la compraventa de joyas y metales, objetos u obras de arte, la cerrajería de seguridad o el comercio al por mayor de chatarra o productos de desecho.

Por otro lado, desde la estricta perspectiva de la seguridad ciudadana, se contempla el régimen de intervención de las autoridades competentes en materia de espectáculos públicos y actividades recreativas, sin perjuicio de las competencias de las comunidades autónomas y de las entidades locales en lo que se refiere a su normal desarrollo.

El capítulo V, que regula el régimen sancionador, introduce novedades relevantes con respecto a la Ley Orgánica 1/1992, de 21 de febrero. La redacción del capítulo en su conjunto tiene en cuenta, como reiteradamente ha declarado el Tribunal Constitucional, que el Derecho administrativo sancionador y el Derecho penal son, con matices, manifestaciones de un único ius puniendi del Estado. Por tanto, la Ley está orientada a dar cumplimiento a los principios que rigen la potestad sancionadora administrativa, singularmente los de responsabilidad, proporcionalidad y legalidad, en sus dos vertientes, de legalidad formal o reserva de Ley y legalidad material o tipicidad, sin perjuicio de la admisión de la colaboración reglamentaria para la especificación de conductas y sanciones en relación con las infracciones tipificadas por la Ley.

En cuanto a los autores de las conductas tipificadas como infracciones, se exime de responsabilidad a los menores de catorce años, en consonancia con la legislación sobre responsabilidad penal del menor. Asimismo se prevé que cuando sea declarado autor de los hechos cometidos un menor de dieciocho años no emancipado o una persona con la capacidad modificada judicialmente responderán solidariamente con él de los daños y perjuicios ocasionados sus padres, tutores, curadores, acogedores o guardadores legales o de hecho.

A fin de garantizar la proporcionalidad en la imposición de las sanciones graves y muy graves previstas en la Ley, se dividen las sanciones pecuniarias en tres tramos de igual extensión, que dan lugar a los grados mínimo, medio y máximo de las mismas y se recogen las circunstancias agravantes y los criterios de graduación que deberán tenerse en cuenta para la individualización de las sanciones pecuniarias, acogiendo así una exigencia del principio de proporcionalidad presente en la jurisprudencia contencioso-administrativa, pero que tiene escaso reflejo en los regímenes sancionadores que incorporan numerosas normas de nuestro ordenamiento jurídico administrativo.

Con respecto al cuadro de infracciones, en aras de un mejor ajuste al principio de tipicidad, se introduce un elenco de conductas que se califican como leves, graves y muy graves, estas últimas ausentes de la Ley Orgánica 1/1992, de 21 de febrero, que simplemente permitía la calificación de determinadas infracciones graves como muy graves en función de las circunstancias concurrentes.

Junto a las infracciones tipificadas por el legislador de 1992, la Ley sanciona conductas que, sin ser constitutivas de delito, atentan gravemente contra la seguridad ciudadana, como son las reuniones o manifestaciones prohibidas en lugares que tengan la condición de infraestructuras e instalaciones en las que se prestan servicios básicos para la comunidad y los actos de intrusión en éstas, cuando se ocasione un riesgo para las personas; la proyección de haces de luz sobre los conductores o pilotos de medios de transporte con riesgo de provocar un accidente, o la celebración de espectáculos públicos o actividades

recreativas a pesar de la prohibición o suspensión acordada por la autoridad por razones de seguridad, entre otras. Se sancionan igualmente conductas que representan un ejercicio extralimitado del derecho de reunión y manifestación, así como la perturbación del ejercicio de este derecho fundamental cuando no constituyan delito. Otras infracciones tienen por objeto preservar el legítimo ejercicio de sus funciones por las autoridades y sus agentes, así como por los servicios de emergencia.

Por otra parte, la reforma en tramitación del Código Penal exige una revisión de las infracciones penales de esta naturaleza que contenía el libro III del código punitivo para incorporar al ámbito administrativo algunas conductas que, de lo contrario, quedarían impunes, como son ciertas alteraciones del orden público, las faltas de respeto a la autoridad, el deslucimiento de determinados bienes en la vía pública o dejar sueltos animales peligrosos. También se recogen las infracciones previstas en la Ley Orgánica 1/1992, de 21 de febrero, relacionadas con el consumo de drogas tóxicas, estupefacientes o sustancias psicotrópicas, a las que se agregan otras dirigidas a favorecerlo. Se ha considerado oportuno sancionar comportamientos atentatorios a la libertad sexual de las personas, especialmente de los menores, o que perturban la convivencia ciudadana o el pacífico disfrute de las vías y espacios públicos, todos ellos bienes jurídicos cuya protección forma parte de los fines de esta Ley por su colindancia con la seguridad ciudadana.

Respecto de las sanciones, se reordenan las pecuniarias y se establecen tres tramos de igual extensión, que dan lugar a los grados mínimo, medio y máximo de las mismas, si bien no se eleva el importe de las que pueden imponerse por la comisión de infracciones muy graves, a pesar del tiempo transcurrido desde la aprobación de la Ley Orgánica 1/1992, de 21 de febrero. Asimismo se ha previsto que cabrá exigir al infractor, en su caso, la reposición de los bienes dañados a su situación originaria o, cuando ello no fuera posible, la indemnización por los daños y perjuicios causados, al igual que también sucede en otros ámbitos en los que se exige una reparación in natura de la situación alterada con el comportamiento infractor y, en su defecto, la satisfacción de un equivalente económico. Y con objeto de dar el tratamiento adecuado a las infracciones de los menores de dieciocho años en materia de consumo o tenencia ilícitos de drogas tóxicas, estupefacientes o sustancias psicotrópicas se prevé la suspensión de la sanción si aquéllos accedan a someterse a tratamiento o rehabilitación, si lo precisan, o a actividades reeducativas.

A fin de contribuir a evitar la proliferación de procedimientos administrativos especiales, se establece que el ejercicio de la potestad sancionadora en materia de protección de la seguridad ciudadana se regirá por la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, y su normativa de desarrollo, sin renunciar a la incorporación de determinadas especialidades, como la regulación de un procedimiento abreviado, que permite satisfacer el pago voluntario de las sanciones pecuniarias por la comisión de infracciones graves o leves en un breve plazo desde su notificación, con el efecto de la reducción del 50 por 100 de su importe, en términos análogos a los ya contemplados en otras normas. Se crea, en fin, un Registro Central de Infracciones contra la Seguridad Ciudadana, indispensable para poder apreciar la reincidencia de los infractores y permitir, de este modo, sancionar adecuadamente a quienes de modo voluntario y reiterado incurren en conductas merecedoras de reproche jurídico.

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

1. La seguridad ciudadana es un requisito indispensable para el pleno ejercicio de los derechos fundamentales y las libertades públicas, y su salvaguarda, como bien jurídico de carácter colectivo, es función del Estado, con sujeción a la Constitución y a las Leyes.

2. Esta Ley tiene por objeto la regulación de un conjunto plural y diversificado de actuaciones de distinta naturaleza orientadas a la tutela de la seguridad ciudadana, mediante la protección de personas y bienes y el mantenimiento de la tranquilidad de los ciudadanos.

Artículo 2. *Ámbito de aplicación.*

1. Las disposiciones de esta Ley son aplicables en todo el territorio nacional, sin perjuicio de las competencias que, en su caso, hayan asumido las comunidades autónomas en el marco de la Constitución, de los estatutos de autonomía y de la legislación del Estado en materia de seguridad pública.

2. En particular, quedan fuera del ámbito de aplicación de esta Ley las prescripciones que tienen por objeto velar por el buen orden de los espectáculos y la protección de las personas y bienes a través de una acción administrativa ordinaria, aun cuando la misma pueda conllevar la intervención de las Fuerzas y Cuerpos de Seguridad, siempre que ésta se conciba como elemento integrante del sistema preventivo habitual del control del espectáculo.

3. Asimismo, esta Ley se aplicará sin menoscabo de los regímenes legales que regulan ámbitos concretos de la seguridad pública, como la seguridad aérea, marítima, ferroviaria, vial o en los transportes, quedando, en todo caso, salvaguardadas las disposiciones referentes a la defensa nacional y la regulación de los estados de alarma, excepción y sitio.

Artículo 3. *Fines.*

Constituyen los fines de esta Ley y de la acción de los poderes públicos en su ámbito de aplicación:

a) La protección del libre ejercicio de los derechos fundamentales y las libertades públicas y los demás derechos reconocidos y amparados por el ordenamiento jurídico.

b) La garantía del normal funcionamiento de las instituciones.

c) La preservación de la seguridad y la convivencia ciudadanas.

d) El respeto a las Leyes, a la paz y a la seguridad ciudadana en el ejercicio de los derechos y libertades.

e) La protección de las personas y bienes, con especial atención a los menores y a las personas con discapacidad necesitadas de especial protección.

f) La pacífica utilización de vías y demás bienes demaniales y, en general, espacios destinados al uso y disfrute público.

g) La garantía de las condiciones de normalidad en la prestación de los servicios básicos para la comunidad.

h) La prevención de la comisión de delitos e infracciones administrativas directamente relacionadas con los fines indicados en los párrafos anteriores y la sanción de las de esta naturaleza tipificadas en esta Ley.

i) La transparencia en la actuación de los poderes públicos en materia de seguridad ciudadana.

Artículo 4. *Principios rectores de la acción de los poderes públicos en relación con la seguridad ciudadana.*

1. El ejercicio de las potestades y facultades reconocidas por esta Ley a las administraciones públicas y, específicamente, a las autoridades y demás órganos competentes en materia de seguridad ciudadana y a los miembros de las Fuerzas y Cuerpos de Seguridad se regirá por los principios de legalidad, igualdad de trato y no discriminación, oportunidad, proporcionalidad, eficacia, eficiencia y responsabilidad, y se someterá al control administrativo y jurisdiccional.

En particular, las disposiciones de los capítulos III y V deberán interpretarse y aplicarse del modo más favorable a la plena efectividad de los derechos fundamentales y libertades públicas, singularmente de los derechos de reunión y manifestación, las libertades de expresión e información, la libertad sindical y el derecho de huelga.

2. En particular, la actuación de los miembros de las Fuerzas y Cuerpos de Seguridad está sujeta a los principios básicos de actuación regulados en el artículo 5 de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad.

3. La actividad de intervención se justifica por la existencia de una amenaza concreta o de un comportamiento objetivamente peligroso que, razonablemente, sea susceptible de provocar un perjuicio real para la seguridad ciudadana y, en concreto, atentar contra los derechos y libertades individuales y colectivos o alterar el normal funcionamiento de las

instituciones públicas. Las concretas intervenciones para el mantenimiento y restablecimiento de la seguridad ciudadana se realizarán conforme a lo dispuesto en el capítulo III de esta Ley.

Artículo 5. *Autoridades y órganos competentes.*

1. Corresponde al Gobierno, a través del Ministerio del Interior y de los demás órganos y autoridades competentes y de las Fuerzas y Cuerpos de Seguridad a sus órdenes, la preparación, dirección y ejecución de la política en relación con la administración general de la seguridad ciudadana, sin perjuicio de las competencias atribuidas a otras administraciones públicas en dicha materia.

2. Son autoridades y órganos competentes en materia de seguridad ciudadana, en el ámbito de la Administración General del Estado:

a) El Ministro del Interior.

b) El Secretario de Estado de Seguridad.

c) Los titulares de los órganos directivos del Ministerio del Interior que tengan atribuida tal condición, en virtud de disposiciones legales o reglamentarias.

d) Los Delegados del Gobierno en las comunidades autónomas y en las Ciudades de Ceuta y Melilla.

e) Los Subdelegados del Gobierno en las provincias y los Directores Insulares.

3. Serán autoridades y órganos competentes, a los efectos de esta Ley, los correspondientes de las comunidades autónomas que hayan asumido competencias para la protección de personas y bienes y para el mantenimiento de la seguridad ciudadana y cuenten con un cuerpo de policía propio.

4. Las autoridades de las Ciudades de Ceuta y Melilla y las autoridades locales ejercerán las facultades que les corresponden, de acuerdo con la Ley Orgánica 2/1986, de 13 de marzo, y la legislación de régimen local, espectáculos públicos, actividades recreativas y actividades clasificadas.

Artículo 6. *Cooperación interadministrativa.*

La Administración General del Estado y las demás administraciones públicas con competencias en materia de seguridad ciudadana se regirán, en sus relaciones, por los principios de cooperación y lealtad institucional, facilitándose la información de acuerdo con la legislación vigente y la asistencia técnica necesarias en el ejercicio de sus respectivas atribuciones, y, cuando fuese preciso, coordinando las acciones destinadas a garantizar el cumplimiento de esta Ley, de conformidad con lo dispuesto en la Ley Orgánica 2/1986, de 13 de marzo, y en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Artículo 7. *Deber de colaboración.*

1. Todas las autoridades y funcionarios públicos, en el ámbito de sus respectivas competencias y de acuerdo con su normativa específica, deberán colaborar con las autoridades y órganos a que se refiere el artículo 5, y prestarles el auxilio que sea posible y adecuado para la consecución de los fines relacionados en el artículo 3. Cuando, por razón de su cargo, tengan conocimiento de hechos que perturben gravemente la seguridad ciudadana o de los que racionalmente pueda inferirse que pueden producir una perturbación grave, estarán obligados a ponerlo inmediatamente en conocimiento de la autoridad competente.

2. Las autoridades y órganos competentes y los miembros de las Fuerzas y Cuerpos de Seguridad podrán recabar de los particulares su ayuda y colaboración en la medida necesaria para el cumplimiento de los fines previstos en esta Ley, especialmente en los casos de grave calamidad pública o catástrofe extraordinaria, siempre que ello no implique riesgo personal para los mismos. Quienes sufran daños y perjuicios por estas causas serán indemnizados de acuerdo con las leyes.

3. Las empresas de seguridad privada, los despachos de detectives privados y el personal de seguridad privada tienen un especial deber de auxiliar a las Fuerzas y Cuerpos

de Seguridad en el ejercicio de sus funciones, prestarles la colaboración que precisen y seguir sus instrucciones, en los términos previstos en la normativa de seguridad privada.

4. El personal que realice funciones de policía administrativa tendrá el especial deber de colaborar en la consecución de los fines previstos en el artículo 3 de esta Ley.

CAPÍTULO II

Documentación e identificación personal

Artículo 8. *Acreditación de la identidad de los ciudadanos españoles.*

1. Los españoles tienen derecho a que se les expida el Documento Nacional de Identidad.

El Documento Nacional de Identidad es un documento público y oficial y tendrá la protección que a estos otorgan las leyes. Es el único documento con suficiente valor por sí solo para la acreditación, a todos los efectos, de la identidad y los datos personales de su titular.

2. En el Documento Nacional de Identidad figurarán la fotografía y la firma de su titular, así como los datos personales que se determinen reglamentariamente, que respetarán el derecho a la intimidad de la persona, sin que en ningún caso, puedan ser relativos a la raza, etnia, religión, creencias, opinión, ideología, discapacidad, orientación o identidad sexual, o afiliación política o sindical. La tarjeta soporte del Documento Nacional de Identidad incorporará las medidas de seguridad necesarias para la consecución de condiciones de calidad e inalterabilidad y máximas garantías para impedir su falsificación.

3. El Documento Nacional de Identidad permite a los españoles mayores de edad que gocen de plena capacidad de obrar y a los menores emancipados la identificación electrónica de su titular, así como la firma electrónica de documentos, en los términos previstos en la legislación específica. Las personas con capacidad modificada judicialmente podrán ejercer esas facultades cuando expresamente lo solicite el interesado y no precise, atendiendo a la resolución judicial que complemente su capacidad, de la representación o asistencia de una institución de protección y apoyo para obligarse o contratar.

El prestador de servicios de certificación procederá a revocar el certificado de firma electrónica a instancia del Ministerio del Interior, tras recibir éste la comunicación del Encargado del Registro Civil de la inscripción de la resolución judicial que determine la necesidad del complemento de la capacidad para obligarse o contratar, del fallecimiento o de la declaración de ausencia o fallecimiento de una persona.

Artículo 9. *Obligaciones y derechos del titular del Documento Nacional de Identidad.*

1. El Documento Nacional de Identidad es obligatorio a partir de los catorce años. Dicho documento es personal e intransferible, debiendo su titular mantenerlo en vigor y conservarlo y custodiarlo con la debida diligencia. No podrá ser privado del mismo, ni siquiera temporalmente, sino en los supuestos en que, conforme a lo previsto por la ley, haya de ser sustituido por otro documento.

2. Todas las personas obligadas a obtener el Documento Nacional de Identidad lo están también a exhibirlo y permitir la comprobación de las medidas de seguridad a las que se refiere el apartado 2 del artículo 8 cuando fueren requeridas para ello por la autoridad o sus agentes, para el cumplimiento de los fines previstos en el apartado 1 del artículo 16. De su sustracción o extravío deberá darse cuenta tan pronto como sea posible a la comisaría de Policía o puesto de las Fuerzas y Cuerpos de Seguridad más próximo.

Artículo 10. *Competencias sobre el Documento Nacional de Identidad.*

1. Corresponde al Ministerio del Interior la competencia exclusiva para la dirección, organización y gestión de todos los aspectos referentes a la confección y expedición del Documento Nacional de Identidad, conforme a lo dispuesto en esta Ley y en la legislación sobre firma electrónica.

2. La competencia a que se refiere el apartado anterior será ejercida por la Dirección General de la Policía, a la que corresponderá también la custodia y responsabilidad de los archivos y ficheros relacionados con el Documento Nacional de Identidad.
3. Su expedición está sujeta al pago de una tasa.

Artículo 11. *Pasaporte de ciudadanos españoles.*

1. El pasaporte español es un documento público, personal, individual e intransferible que, salvo prueba en contrario, acredita la identidad y nacionalidad de los ciudadanos españoles fuera de España, y dentro del territorio nacional, las mismas circunstancias de los españoles no residentes.
2. Los ciudadanos españoles tienen derecho a que les sea expedido el pasaporte, que sólo podrá ser exceptuado en las siguientes circunstancias:

a) Haber sido condenado a penas o medidas de seguridad privativas de libertad, mientras no se hayan extinguido, salvo que obtenga autorización del órgano judicial competente.
b) Haber sido acordada por el órgano judicial competente la retirada de su pasaporte de acuerdo con lo previsto por la ley.
c) Haberle sido impuesta una medida de libertad vigilada con prohibición de abandonar el territorio nacional, salvo que obtenga autorización del órgano judicial competente.
d) Cuando el órgano judicial competente haya prohibido la salida de España o la expedición de pasaporte al menor de edad o a la persona con la capacidad modificada judicialmente, de acuerdo con lo dispuesto por la ley.

3. La obtención del pasaporte por los ciudadanos sujetos a patria potestad o a tutela estará condicionada al consentimiento expreso de las personas u órgano que tenga encomendado su ejercicio o, en su defecto, del órgano judicial competente.
4. Los titulares del pasaporte tienen la obligación de exhibirlo y facilitarlo cuando fuesen requeridos para ello por la autoridad o sus agentes. También estarán obligados a su custodia y conservación con la debida diligencia. De su sustracción o extravío deberá darse cuenta de manera inmediata a las Fuerzas y Cuerpos de Seguridad o, en su caso, a la Representación Diplomática o Consular de España en el extranjero.

Artículo 12. *Competencias sobre el pasaporte.*

1. La competencia para su expedición corresponde:

a) En el territorio nacional, a la Dirección General de la Policía.
b) En el extranjero, a las Representaciones Diplomáticas y Consulares de España.

2. Su expedición está sujeta al pago de una tasa.
3. Corresponde al Gobierno, a propuesta de los Ministros del Interior y de Asuntos Exteriores y de Cooperación, desarrollar esta Ley en lo referente al régimen jurídico del pasaporte.

Artículo 13. *Acreditación de la identidad de ciudadanos extranjeros.*

1. Los extranjeros que se encuentren en territorio español tienen el derecho y la obligación de conservar y portar consigo la documentación que acredite su identidad expedida por las autoridades competentes del país de origen o de procedencia, así como la que acredite su situación regular en España.
2. Los extranjeros no podrán ser privados de su documentación de origen, salvo en el curso de investigaciones judiciales de carácter penal.
3. Los extranjeros estarán obligados a exhibir la documentación mencionada en el apartado 1 de este artículo y permitir la comprobación de las medidas de seguridad de la misma, cuando fueran requeridos por las autoridades o sus agentes de conformidad con lo dispuesto en la ley, y por el tiempo imprescindible para dicha comprobación, sin perjuicio de poder demostrar su identidad por cualquier otro medio si no la llevaran consigo.

CAPÍTULO III

Actuaciones para el mantenimiento y restablecimiento de la seguridad ciudadana

Sección 1.ª Potestades generales de policía de seguridad

Artículo 14. *Órdenes y prohibiciones.*

Las autoridades competentes, de conformidad con las Leyes y reglamentos, podrán dictar las órdenes y prohibiciones y disponer las actuaciones policiales estrictamente necesarias para asegurar la consecución de los fines previstos en esta Ley, mediante resolución debidamente motivada.

Artículo 15. *Entrada y registro en domicilio y edificios de organismos oficiales.*

1. Los agentes de las Fuerzas y Cuerpos de Seguridad sólo podrán proceder a la entrada y registro en domicilio en los casos permitidos por la Constitución y en los términos que fijen las Leyes.
2. Será causa legítima suficiente para la entrada en domicilio la necesidad de evitar daños inminentes y graves a las personas y a las cosas, en supuestos de catástrofe, calamidad, ruina inminente u otros semejantes de extrema y urgente necesidad.
3. Para la entrada en edificios ocupados por organismos oficiales o entidades públicas, no será preciso el consentimiento de la autoridad o funcionario que los tuviere a su cargo.
4. Cuando por las causas previstas en este artículo las Fuerzas y Cuerpos de Seguridad entren en un domicilio particular, remitirán sin dilación el acta o atestado que instruyan a la autoridad judicial competente.

Artículo 16. *Identificación de personas.*

1. En el cumplimiento de sus funciones de indagación y prevención delictiva, así como para la sanción de infracciones penales y administrativas, los agentes de las Fuerzas y Cuerpos de Seguridad podrán requerir la identificación de las personas en los siguientes supuestos:

a) Cuando existan indicios de que han podido participar en la comisión de una infracción.
b) Cuando, en atención a las circunstancias concurrentes, se considere razonablemente necesario que acrediten su identidad para prevenir la comisión de un delito.

En estos supuestos, los agentes podrán realizar las comprobaciones necesarias en la vía pública o en el lugar donde se hubiese hecho el requerimiento, incluida la identificación de las personas cuyo rostro no sea visible total o parcialmente por utilizar cualquier tipo de prenda u objeto que lo cubra, impidiendo o dificultando la identificación, cuando fuere preciso a los efectos indicados.

En la práctica de la identificación se respetarán estrictamente los principios de proporcionalidad, igualdad de trato y no discriminación por razón de nacimiento, nacionalidad, origen racial o étnico, sexo, religión o creencias, edad, discapacidad, orientación o identidad sexual, opinión o cualquier otra condición o circunstancia personal o social.

2. Cuando no fuera posible la identificación por cualquier medio, incluida la vía telemática o telefónica, o si la persona se negase a identificarse, los agentes, para impedir la comisión de un delito o al objeto de sancionar una infracción, podrán requerir a quienes no pudieran ser identificados a que les acompañen a las dependencias policiales más próximas en las que se disponga de los medios adecuados para la práctica de esta diligencia, a los solos efectos de su identificación y por el tiempo estrictamente necesario, que en ningún caso podrá superar las seis horas.

La persona a la que se solicite que se identifique será informada de modo inmediato y comprensible de las razones de dicha solicitud, así como, en su caso, del requerimiento para que acompañe a los agentes a las dependencias policiales.

3. En las dependencias a que se hace referencia en el apartado 2 se llevará un libro-registro en el que sólo se practicarán asientos relacionados con la seguridad ciudadana.

Constarán en él las diligencias de identificación practicadas, así como los motivos, circunstancias y duración de las mismas, y sólo podrán ser comunicados sus datos a la autoridad judicial competente y al Ministerio Fiscal. El órgano competente de la Administración remitirá mensualmente al Ministerio Fiscal extracto de las diligencias de identificación con expresión del tiempo utilizado en cada una. Los asientos de este libro-registro se cancelarán de oficio a los tres años.

4. A las personas desplazadas a dependencias policiales a efectos de identificación, se les deberá expedir a su salida un volante acreditativo del tiempo de permanencia en ellas, la causa y la identidad de los agentes actuantes.

5. En los casos de resistencia o negativa a identificarse o a colaborar en las comprobaciones o prácticas de identificación, se estará a lo dispuesto en el Código Penal, en la Ley de Enjuiciamiento Criminal y, en su caso, en esta Ley.

Artículo 17. *Restricción del tránsito y controles en las vías públicas.*

1. Los agentes de las Fuerzas y Cuerpos de Seguridad podrán limitar o restringir la circulación o permanencia en vías o lugares públicos y establecer zonas de seguridad en supuestos de alteración de la seguridad ciudadana o de la pacífica convivencia, o cuando existan indicios racionales de que pueda producirse dicha alteración, por el tiempo imprescindible para su mantenimiento o restablecimiento. Asimismo podrán ocupar preventivamente los efectos o instrumentos susceptibles de ser utilizados para acciones ilegales, dándoles el destino que legalmente proceda.

2. Para la prevención de delitos de especial gravedad o generadores de alarma social, así como para el descubrimiento y detención de quienes hubieran participado en su comisión y proceder a la recogida de los instrumentos, efectos o pruebas, se podrán establecer controles en las vías, lugares o establecimientos públicos, siempre que resulte indispensable proceder a la identificación de personas que se encuentren en ellos, al registro de vehículos o al control superficial de efectos personales.

Artículo 18. *Comprobaciones y registros en lugares públicos.*

1. Los agentes de la autoridad podrán practicar las comprobaciones en las personas, bienes y vehículos que sean necesarias para impedir que en las vías, lugares y establecimientos públicos se porten o utilicen ilegalmente armas, explosivos, sustancias peligrosas u otros objetos, instrumentos o medios que generen un riesgo potencialmente grave para las personas, susceptibles de ser utilizados para la comisión de un delito o alterar la seguridad ciudadana, cuando tengan indicios de su eventual presencia en dichos lugares, procediendo, en su caso, a su intervención. A tal fin, los ciudadanos tienen el deber de colaborar y no obstaculizar la labor de los agentes de la autoridad en el ejercicio de sus funciones.

2. Los agentes de la autoridad podrán proceder a la ocupación temporal de cualesquiera objetos, instrumentos o medios de agresión, incluso de las armas que se porten con licencia, permiso o autorización si se estima necesario, con objeto de prevenir la comisión de cualquier delito, o cuando exista peligro para la seguridad de las personas o de los bienes.

Artículo 19. *Disposiciones comunes a las diligencias de identificación, registro y comprobación.*

1. Las diligencias de identificación, registro y comprobación practicadas por los agentes de las Fuerzas y Cuerpos de Seguridad con ocasión de actuaciones realizadas conforme a lo dispuesto en esta sección no estarán sujetas a las mismas formalidades que la detención.

2. La aprehensión durante las diligencias de identificación, registro y comprobación de armas, drogas tóxicas, estupefacientes, sustancias psicotrópicas u otros efectos procedentes de un delito o infracción administrativa se hará constar en el acta correspondiente, que habrá de ser firmada por el interesado; si éste se negara a firmarla, se dejará constancia expresa de su negativa. El acta que se extienda gozará de presunción de veracidad de los hechos en ella consignados, salvo prueba en contrario.

Artículo 20. *Registros corporales externos.*

1. Podrá practicarse el registro corporal externo y superficial de la persona cuando existan indicios racionales para suponer que puede conducir al hallazgo de instrumentos, efectos u otros objetos relevantes para el ejercicio de las funciones de indagación y prevención que encomiendan las leyes a las Fuerzas y Cuerpos de Seguridad.

2. Salvo que exista una situación de urgencia por riesgo grave e inminente para los agentes:

a) El registro se realizará por un agente del mismo sexo que la persona sobre la que se practique esta diligencia.

b) Y si exigiera dejar a la vista partes del cuerpo normalmente cubiertas por ropa, se efectuará en un lugar reservado y fuera de la vista de terceros. Se dejará constancia escrita de esta diligencia, de sus causas y de la identidad del agente que la adoptó.

3. Los registros corporales externos respetarán los principios del apartado 1 del artículo 16, así como el de injerencia mínima, y se realizarán del modo que cause el menor perjuicio a la intimidad y dignidad de la persona afectada, que será informada de modo inmediato y comprensible de las razones de su realización.

4. Los registros a los que se refiere este artículo podrán llevarse a cabo contra la voluntad del afectado, adoptando las medidas de compulsión indispensables, conforme a los principios de idoneidad, necesidad y proporcionalidad.

Artículo 21. *Medidas de seguridad extraordinarias.*

Las autoridades competentes podrán acordar, como medidas de seguridad extraordinarias, el cierre o desalojo de locales o establecimientos, la prohibición del paso, la evacuación de inmuebles o espacios públicos debidamente acotados, o el depósito de explosivos u otras sustancias susceptibles de ser empleadas como tales, en situaciones de emergencia que las hagan imprescindibles y durante el tiempo estrictamente necesario para garantizar la seguridad ciudadana. Dichas medidas podrán adoptarse por los agentes de la autoridad si la urgencia de la situación lo hiciera imprescindible, incluso mediante órdenes verbales.

A los efectos de este artículo, se entiende por emergencia aquella situación de riesgo sobrevenida por un evento que pone en peligro inminente a personas o bienes y exige una actuación rápida por parte de la autoridad o de sus agentes para evitarla o mitigar sus efectos.

Artículo 22. *Uso de videocámaras.*

La autoridad gubernativa y, en su caso, las Fuerzas y Cuerpos de Seguridad podrán proceder a la grabación de personas, lugares u objetos mediante cámaras de videovigilancia fijas o móviles legalmente autorizadas, de acuerdo con la legislación vigente en la materia.

Sección 2.ª Mantenimiento y restablecimiento de la seguridad ciudadana en reuniones y manifestaciones

Artículo 23. *Reuniones y manifestaciones.*

1. Las autoridades a las que se refiere esta Ley adoptarán las medidas necesarias para proteger la celebración de reuniones y manifestaciones, impidiendo que se perturbe la seguridad ciudadana.

Asimismo podrán acordar la disolución de reuniones en lugares de tránsito público y manifestaciones en los supuestos previstos en el artículo 5 de la Ley Orgánica 9/1983, de 15 de julio, reguladora del derecho de reunión.

También podrán disolver las concentraciones de vehículos en las vías públicas y retirar aquéllos o cualesquiera otra clase de obstáculos cuando impidieran, pusieran en peligro o dificultaran la circulación por dichas vías.

2. Las medidas de intervención para el mantenimiento o el restablecimiento de la seguridad ciudadana en reuniones y manifestaciones serán graduales y proporcionadas a las circunstancias. La disolución de reuniones y manifestaciones constituirá el último recurso.

3. Antes de adoptar las medidas a las que se refiere el apartado anterior, las unidades actuantes de las Fuerzas y Cuerpos de Seguridad deberán avisar de tales medidas a las personas afectadas, pudiendo hacerlo de manera verbal si la urgencia de la situación lo hiciera imprescindible.

En caso de que se produzca una alteración de la seguridad ciudadana con armas, artefactos explosivos u objetos contundentes o de cualquier otro modo peligrosos, las Fuerzas y Cuerpos de Seguridad podrán disolver la reunión o manifestación o retirar los vehículos y obstáculos sin necesidad de previo aviso.

Artículo 24. *Colaboración entre las Fuerzas y Cuerpos de Seguridad.*

En los casos a que se refiere el artículo anterior, las Fuerzas y Cuerpos de Seguridad colaborarán mutuamente en los términos previstos en su Ley orgánica reguladora.

CAPÍTULO IV

Potestades especiales de policía administrativa de seguridad

Artículo 25. *Obligaciones de registro documental.*

1. Las personas físicas o jurídicas que ejerzan actividades relevantes para la seguridad ciudadana, como las de hospedaje, transporte de personas, acceso comercial a servicios telefónicos o telemáticos de uso público mediante establecimientos abiertos al público, comercio o reparación de objetos usados, alquiler o desguace de vehículos de motor, compraventa de joyas y metales, ya sean preciosos o no, objetos u obras de arte, cerrajería de seguridad, centros gestores de residuos metálicos, establecimientos de comercio al por mayor de chatarra o productos de desecho, o de venta de productos químicos peligrosos a particulares, quedarán sujetas a las obligaciones de registro documental e información en los términos que establezcan las disposiciones aplicables.

2. Los titulares de embarcaciones de alta velocidad, así como los de aeronaves ligeras estarán obligados a realizar las actuaciones de registro documental e información previstas en la normativa vigente.

Artículo 26. *Establecimientos e instalaciones obligados a adoptar medidas de seguridad.*

Reglamentariamente, en desarrollo de lo dispuesto en esta Ley, en la legislación de seguridad privada, en la de infraestructuras críticas o en otra normativa sectorial, podrá establecerse la necesidad de adoptar medidas de seguridad en establecimientos e instalaciones industriales, comerciales y de servicios, así como en las infraestructuras críticas, con la finalidad de prevenir la comisión de actos delictivos o infracciones administrativas, o cuando generen riesgos directos para terceros o sean especialmente vulnerables.

Artículo 27. *Espectáculos y actividades recreativas.*

1. El Estado podrá dictar normas de seguridad pública para los edificios e instalaciones en los que se celebren espectáculos y actividades recreativas.

2. Las autoridades a las que se refiere esta Ley adoptarán las medidas necesarias para preservar la pacífica celebración de espectáculos públicos. En particular, podrán prohibir y, en caso de estar celebrándose, suspender los espectáculos y actividades recreativas cuando exista un peligro cierto para personas y bienes, o acaecieran o se previeran graves alteraciones de la seguridad ciudadana.

3. La normativa específica determinará los supuestos en los que los delegados de la autoridad deban estar presentes en la celebración de los espectáculos y actividades recreativas, los cuales podrán proceder, previo aviso a los organizadores, a la suspensión de los mismos por razones de máxima urgencia en los supuestos previstos en el apartado anterior.

4. Los espectáculos deportivos quedarán, en todo caso, sujetos a las medidas de prevención de la violencia dispuestas en la legislación específica contra la violencia, el racismo, la xenofobia y la intolerancia en el deporte.

Artículo 28. *Control administrativo sobre armas, explosivos, cartuchería y artículos pirotécnicos.*

1. Corresponde al Gobierno:

a) La regulación de los requisitos y condiciones de fabricación, reparación, circulación, almacenamiento, comercio, adquisición, enajenación, tenencia y utilización de armas, sus imitaciones, réplicas y piezas fundamentales.
b) La regulación de los requisitos y condiciones mencionados anteriormente en relación con los explosivos, cartuchería y artículos pirotécnicos.
c) La adopción de las medidas de control necesarias para el cumplimiento de los requisitos y condiciones a que se refieren los párrafos a) y b).

2. La intervención de armas, explosivos, cartuchería y artículos pirotécnicos corresponde al Ministerio del Interior, que la ejerce a través de la Dirección General de la Guardia Civil, cuyos servicios están habilitados para realizar en cualquier momento las inspecciones y comprobaciones que sean necesarias en los espacios que estén destinados a su fabricación, depósito, comercialización o utilización.

Artículo 29. *Medidas de control.*

1. El Gobierno regulará las medidas de control necesarias sobre las materias relacionadas en el artículo anterior:

a) Mediante la sujeción de la apertura y funcionamiento de las fábricas, talleres, depósitos, establecimientos de comercialización y lugares de utilización y las actividades relacionadas con ellas a requisitos de catalogación o clasificación, autorización, información, inspección, vigilancia y control, requisitos especiales de habilitación para el personal encargado de su manipulación, así como la determinación del régimen de responsabilidad de quienes tengan el deber de prevenir la comisión de determinadas infracciones.
b) Estableciendo la obligatoria titularidad de licencias, permisos o autorizaciones para la adquisición, tenencia y utilización de armas de fuego, cuya expedición tendrá carácter restrictivo cuando se trate de armas de defensa personal, en relación con las cuales la concesión de las licencias, permisos o autorizaciones se limitará a supuestos de estricta necesidad. Para la concesión de licencias, permisos y autorizaciones se tendrán en cuenta la conducta y antecedentes del interesado. En todo caso, el solicitante prestará su consentimiento expreso a favor del órgano de la Administración General del Estado que tramita su solicitud para que se recaben sus antecedentes penales.
c) A través de la prohibición de la fabricación, tenencia y comercialización de armas, cartuchería, artículos pirotécnicos y explosivos especialmente peligrosos, así como el depósito de los mismos.

2. La fabricación, comercio y distribución de armas, artículos pirotécnicos, cartuchería y explosivos, constituye un sector con regulación específica en materia de derecho de establecimiento, en los términos previstos por la legislación sobre inversiones extranjeras en España, correspondiendo a los Ministerios de Defensa, del Interior y de Industria, Energía y Turismo el ejercicio de las competencias de supervisión y control.

CAPÍTULO V

Régimen sancionador

Sección 1.ª Sujetos responsables, órganos competentes y reglas generales sobre las infracciones y la aplicación de las sanciones

Artículo 30. *Sujetos responsables.*

1. La responsabilidad por las infracciones cometidas recaerá directamente en el autor del hecho en que consista la infracción.
2. Estarán exentos de responsabilidad por las infracciones cometidas los menores de catorce años.

En caso de que la infracción sea cometida por un menor de catorce años, la autoridad competente lo pondrá en conocimiento del Ministerio Fiscal para que inicie, en su caso, las actuaciones oportunas.

3. A los efectos de esta Ley se considerarán organizadores o promotores de las reuniones en lugares de tránsito público o manifestaciones las personas físicas o jurídicas que hayan suscrito la preceptiva comunicación. Asimismo, aun no habiendo suscrito o presentado la comunicación, también se considerarán organizadores o promotores quienes de hecho las presidan, dirijan o ejerzan actos semejantes, o quienes por publicaciones o declaraciones de convocatoria de las mismas, por las manifestaciones orales o escritas que en ellas se difundan, por los lemas, banderas u otros signos que ostenten o por cualesquiera otros hechos pueda determinarse razonablemente que son directores de aquellas.

Artículo 31. *Normas concursales.*

1. Los hechos susceptibles de ser calificados con arreglo a dos o más preceptos de esta u otra Ley se sancionarán observando las siguientes reglas:

a) El precepto especial se aplicará con preferencia al general.

b) El precepto más amplio o complejo absorberá el que sancione las infracciones consumidas en aquel.

c) En defecto de los criterios anteriores, el precepto más grave excluirá los que sancionen el hecho con una sanción menor.

2. En el caso de que un solo hecho constituya dos o más infracciones, o cuando una de ellas sea medio necesario para cometer la otra, la conducta será sancionada por aquella infracción que aplique una mayor sanción.

3. Cuando una acción u omisión deba tomarse en consideración como criterio de graduación de la sanción o como circunstancia que determine la calificación de la infracción no podrá ser sancionada como infracción independiente.

Artículo 32. *Órganos competentes.*

1. Son órganos competentes en el ámbito de la Administración General del Estado:

a) El Ministro del Interior, para la sanción de las infracciones muy graves en grado máximo.

b) El Secretario de Estado de Seguridad, para la sanción de infracciones muy graves en grado medio y en grado mínimo.

c) Los Delegados del Gobierno en las comunidades autónomas y en las Ciudades de Ceuta y Melilla, para la sanción de las infracciones graves y leves.

2. Serán competentes para imponer las sanciones tipificadas en esta Ley las autoridades correspondientes de la Comunidad Autónoma en el ámbito de sus competencias en materia de seguridad ciudadana.

3. Los alcaldes podrán imponer las sanciones y adoptar las medidas previstas en esta Ley cuando las infracciones se cometieran en espacios públicos municipales o afecten a bienes de titularidad local, siempre que ostenten competencia sobre la materia de acuerdo con la legislación específica.

En los términos del artículo 41, las ordenanzas municipales podrán introducir especificaciones o graduaciones en el cuadro de las infracciones y sanciones tipificadas en esta Ley.

Artículo 33. *Graduación de las sanciones.*

1. En la imposición de las sanciones por la comisión de las infracciones tipificadas en esta Ley se observará el principio de proporcionalidad, de acuerdo con lo dispuesto en los apartados siguientes.

2. Dentro de los límites previstos para las infracciones muy graves y graves, las multas se dividirán en tres tramos de igual extensión, correspondientes a los grados mínimo, medio y máximo, en los términos del apartado 1 del artículo 39.

La comisión de una infracción determinará la imposición de la multa correspondiente en grado mínimo.

La infracción se sancionará con multa en grado medio cuando se acredite la concurrencia, al menos, de una de las siguientes circunstancias:

a) La reincidencia, por la comisión en el término de dos años de más de una infracción de la misma naturaleza, cuando así haya sido declarado por resolución firme en vía administrativa.

b) La realización de los hechos interviniendo violencia, amenaza o intimidación.

c) La ejecución de los hechos usando cualquier tipo de prenda u objeto que cubra el rostro, impidiendo o dificultando la identificación.

d) Que en la comisión de la infracción se utilice a menores de edad, personas con discapacidad necesitadas de especial protección o en situación de vulnerabilidad.

En cada grado, para la individualización de la multa se tendrán en cuenta los siguientes criterios:

a) La entidad del riesgo producido para la seguridad ciudadana o la salud pública.

b) La cuantía del perjuicio causado.

c) La trascendencia del perjuicio para la prevención, mantenimiento o restablecimiento de la seguridad ciudadana.

d) La alteración ocasionada en el funcionamiento de los servicios públicos o en el abastecimiento a la población de bienes y servicios.

e) El grado de culpabilidad.

f) El beneficio económico obtenido como consecuencia de la comisión de la infracción.

g) La capacidad económica del infractor.

Las infracciones sólo se sancionarán con multa en grado máximo cuando los hechos revistan especial gravedad y así se justifique teniendo en cuenta el número y la entidad de las circunstancias concurrentes y los criterios previstos en este apartado.

3. La multa por la comisión de infracciones leves se determinará directamente atendiendo a las circunstancias y los criterios del apartado anterior.

Sección 2.ª Infracciones y sanciones

Artículo 34. *Clasificación de las infracciones.*

Las infracciones tipificadas en esta Ley se clasifican en muy graves, graves y leves.

Artículo 35. *Infracciones muy graves.*

Son infracciones muy graves:

1. Las reuniones o manifestaciones no comunicadas o prohibidas en infraestructuras o instalaciones en las que se prestan servicios básicos para la comunidad o en sus inmediaciones, así como la intrusión en los recintos de éstas, incluido su sobrevuelo, cuando, en cualquiera de estos supuestos, se haya generado un riesgo para la vida o la integridad física de las personas.

En el caso de las reuniones y manifestaciones serán responsables los organizadores o promotores.

2. La fabricación, reparación, almacenamiento, circulación, comercio, transporte, distribución, adquisición, certificación, enajenación o utilización de armas reglamentarias, explosivos catalogados, cartuchería o artículos pirotécnicos, incumpliendo la normativa de aplicación, careciendo de la documentación o autorización requeridas o excediendo los límites autorizados cuando tales conductas no sean constitutivas de delito así como la omisión, insuficiencia, o falta de eficacia de las medidas de seguridad o precauciones que resulten obligatorias, siempre que en tales actuaciones se causen perjuicios muy graves.

3. La celebración de espectáculos públicos o actividades recreativas quebrantando la prohibición o suspensión ordenada por la autoridad correspondiente por razones de seguridad pública.

4. La proyección de haces de luz, mediante cualquier tipo de dispositivo, sobre los pilotos o conductores de medios de transporte que puedan deslumbrarles o distraer su atención y provocar accidentes.

Artículo 36. *Infracciones graves.*

Son infracciones graves:

1. La perturbación de la seguridad ciudadana en actos públicos, espectáculos deportivos o culturales, solemnidades y oficios religiosos u otras reuniones a las que asistan numerosas personas, cuando no sean constitutivas de infracción penal.

2. La perturbación grave de la seguridad ciudadana que se produzca con ocasión de reuniones o manifestaciones frente a las sedes del Congreso de los Diputados, el Senado y las asambleas legislativas de las comunidades autónomas, aunque no estuvieran reunidas, cuando no constituya infracción penal.

3. Causar desórdenes en las vías, espacios o establecimientos públicos, u obstaculizar la vía pública con mobiliario urbano, vehículos, contenedores, neumáticos u otros objetos, cuando en ambos casos se ocasione una alteración grave de la seguridad ciudadana.

4. Los actos de obstrucción que pretendan impedir a cualquier autoridad, empleado público o corporación oficial el ejercicio legítimo de sus funciones, el cumplimiento o la ejecución de acuerdos o resoluciones administrativas o judiciales, siempre que se produzcan al margen de los procedimientos legalmente establecidos y no sean constitutivos de delito.

5. Las acciones y omisiones que impidan u obstaculicen el funcionamiento de los servicios de emergencia, provocando o incrementando un riesgo para la vida o integridad de las personas o de daños en los bienes, o agravando las consecuencias del suceso que motive la actuación de aquéllos.

6. La desobediencia o la resistencia a la autoridad o a sus agentes en el ejercicio de sus funciones, cuando no sean constitutivas de delito, así como la negativa a identificarse a requerimiento de la autoridad o de sus agentes o la alegación de datos falsos o inexactos en los procesos de identificación.

7. La negativa a la disolución de reuniones y manifestaciones en lugares de tránsito público ordenada por la autoridad competente cuando concurran los supuestos del artículo 5 de la Ley Orgánica 9/1983, de 15 de julio.

8. La perturbación del desarrollo de una reunión o manifestación lícita, cuando no constituya infracción penal.

9. La intrusión en infraestructuras o instalaciones en las que se prestan servicios básicos para la comunidad, incluyendo su sobrevuelo, cuando se haya producido una interferencia grave en su funcionamiento.

10. Portar, exhibir o usar armas prohibidas, así como portar, exhibir o usar armas de modo negligente, temerario o intimidatorio, o fuera de los lugares habilitados para su uso, aún cuando en este último caso se tuviera licencia, siempre que dichas conductas no constituyan infracción penal.

11. La solicitud o aceptación por el demandante de servicios sexuales retribuidos en zonas de tránsito público en las proximidades de lugares destinados a su uso por menores, como centros educativos, parques infantiles o espacios de ocio accesibles a menores de edad, o cuando estas conductas, por el lugar en que se realicen, puedan generar un riesgo para la seguridad vial.

Los agentes de la autoridad requerirán a las personas que ofrezcan estos servicios para que se abstengan de hacerlo en dichos lugares, informándoles de que la inobservancia de dicho requerimiento podría constituir una infracción del párrafo 6 de este artículo.

12. La fabricación, reparación, almacenamiento, circulación, comercio, transporte, distribución, adquisición, certificación, enajenación o utilización de armas reglamentarias, explosivos catalogados, cartuchería o artículos pirotécnicos, incumpliendo la normativa de aplicación, careciendo de la documentación o autorización requeridas o excediendo los límites autorizados cuando tales conductas no sean constitutivas de delito, así como la omisión, insuficiencia, o falta de eficacia de las medidas de seguridad o precauciones que resulten obligatorias.

13. La negativa de acceso o la obstrucción deliberada de las inspecciones o controles reglamentarios, establecidos conforme a lo dispuesto en esta Ley, en fábricas, locales, establecimientos, embarcaciones y aeronaves.

14. El uso público e indebido de uniformes, insignias o condecoraciones oficiales, o réplicas de los mismos, así como otros elementos del equipamiento de los cuerpos policiales o de los servicios de emergencia que puedan generar engaño acerca de la condición de quien los use, cuando no sea constitutivo de infracción penal.

15. La falta de colaboración con las Fuerzas y Cuerpos de Seguridad en la averiguación de delitos o en la prevención de acciones que puedan poner en riesgo la seguridad ciudadana en los supuestos previstos en el artículo 7.

16. El consumo o la tenencia ilícitos de drogas tóxicas, estupefacientes o sustancias psicotrópicas, aunque no estuvieran destinadas al tráfico, en lugares, vías, establecimientos públicos o transportes colectivos, así como el abandono de los instrumentos u otros efectos empleados para ello en los citados lugares.

17. El traslado de personas, con cualquier tipo de vehículo, con el objeto de facilitar a éstas el acceso a drogas tóxicas, estupefacientes o sustancias psicotrópicas, siempre que no constituya delito.

18. La ejecución de actos de plantación y cultivo ilícitos de drogas tóxicas, estupefacientes o sustancias psicotrópicas en lugares visibles al público, cuando no sean constitutivos de infracción penal.

19. La tolerancia del consumo ilegal o el tráfico de drogas tóxicas, estupefacientes o sustancias psicotrópicas en locales o establecimientos públicos o la falta de diligencia en orden a impedirlos por parte de los propietarios, administradores o encargados de los mismos.

20. La carencia de los registros previstos en esta Ley para las actividades con trascendencia para la seguridad ciudadana o la omisión de comunicaciones obligatorias.

21. La alegación de datos o circunstancias falsos para la obtención de las documentaciones previstas en esta Ley, siempre que no constituya infracción penal.

22. El incumplimiento de las restricciones a la navegación reglamentariamente impuestas a las embarcaciones de alta velocidad y aeronaves ligeras.

> Téngase en cuenta que se declara que el apartado 22 no es inconstitucional siempre que se interprete que la conducta que tipifica consiste en (i) el incumplimiento de las restricciones a la navegación en esos sectores impuestas por motivos de seguridad ciudadana (ii) que produjese como resultado un perjuicio real para la seguridad ciudadana o una amenaza concreta de la que razonablemente se pueda seguir aquel perjuicio, por la Sentencia del TC 13/2021, de 28 de enero. Ref. BOE-A-2021-2832

23. El uso **no autorizado** de imágenes o datos personales o profesionales de autoridades o miembros de las Fuerzas y Cuerpos de Seguridad que pueda poner en peligro la seguridad personal o familiar de los agentes, de las instalaciones protegidas o en riesgo el éxito de una operación, con respeto al derecho fundamental a la información.

> Téngase en cuenta que se declara la inconstitucionalidad y nulidad del inciso destacado del apartado 23 y la no inconstitucionalidad del resto del apartado siempre que se interprete en el sentido establecido en el FJ 7 C), por la Sentencia del TC 172/2020, de 19 de noviembre. Ref. BOE-A-2020-16819
>
> Asimismo, se declara que el apartado 23 no es inconstitucional siempre que se interprete en el sentido establecido en el fundamento jurídico 2.c) por la Sentencia del TC 13/2021, de 28 de enero. Ref. BOE-A-2021-2832

Artículo 37. *Infracciones leves.*

Son infracciones leves:

1. La celebración de reuniones en lugares de tránsito público o de manifestaciones, incumpliendo lo preceptuado en los artículos 4.2, 8, 9, 10 y 11 de la Ley Orgánica 9/1983, de 15 de julio, cuya responsabilidad corresponderá a los organizadores o promotores.

2. La exhibición de objetos peligrosos para la vida e integridad física de las personas con ánimo intimidatorio, siempre que no constituya delito o infracción grave.

3. El incumplimiento de las restricciones de circulación peatonal o itinerario con ocasión de un acto público, reunión o manifestación, cuando provoquen alteraciones menores en el normal desarrollo de los mismos.

4. Las faltas de respeto y consideración cuyo destinatario sea un miembro de las Fuerzas y Cuerpos de Seguridad en el ejercicio de sus funciones de protección de la seguridad, cuando estas conductas no sean constitutivas de infracción penal.

5. La realización o incitación a la realización de actos que atenten contra la libertad e indemnidad sexual, o ejecutar actos de exhibición obscena, cuando no constituya infracción penal.

6. La proyección de haces de luz, mediante cualquier tipo de dispositivo, sobre miembros de las Fuerzas y Cuerpos de Seguridad para impedir o dificultar el ejercicio de sus funciones.

7. La ocupación de cualquier inmueble, vivienda o edificio ajenos, o la permanencia en ellos, en ambos casos contra la voluntad de su propietario, arrendatario o titular de otro derecho sobre el mismo, cuando no sean constitutivas de infracción penal.

Asimismo la ocupación de la vía pública con infracción de lo dispuesto por la Ley o contra la decisión adoptada en aplicación de aquella por la autoridad competente. Se entenderá incluida en este supuesto la ocupación de la vía pública para la venta ambulante no autorizada.

> Téngase en cuenta que se declara que no son inconstitucionales los apartados 3 y 7 siempre que se interpreten en el sentido establecido en el FJ 6 E) y 6 F), respectivamente, por la Sentencia del TC 172/2020, de 19 de noviembre. Ref. BOE-A-2020-16819
>
> Asimismo, se declara que el apartado 7 no es inconstitucional, siempre que se interprete en el sentido establecido en el fundamento jurídico 2.d) por la Sentencia del TC 13/2021, de 28 de enero. Ref. BOE-A-2021-2832

8. La omisión o la insuficiencia de medidas para garantizar la conservación de la documentación de armas y explosivos, así como la falta de denuncia de la pérdida o sustracción de la misma.

9. Las irregularidades en la cumplimentación de los registros previstos en esta Ley con trascendencia para la seguridad ciudadana, incluyendo la alegación de datos o circunstancias falsos o la omisión de comunicaciones obligatorias dentro de los plazos establecidos, siempre que no constituya infracción penal.

10. El incumplimiento de la obligación de obtener la documentación personal legalmente exigida, así como la omisión negligente de la denuncia de su sustracción o extravío.

11. La negligencia en la custodia y conservación de la documentación personal legalmente exigida, considerándose como tal la tercera y posteriores pérdidas o extravíos en el plazo de un año.

12. La negativa a entregar la documentación personal legalmente exigida cuando se hubiese acordado su retirada o retención.

13. Los daños o el deslucimiento de bienes muebles o inmuebles de uso o servicio público, así como de bienes muebles o inmuebles privados en la vía pública, cuando no constituyan infracción penal.

14. El escalamiento de edificios o monumentos sin autorización cuando exista un riesgo cierto de que se ocasionen daños a las personas o a los bienes.

15. La remoción de vallas, encintados u otros elementos fijos o móviles colocados por las Fuerzas y Cuerpos de Seguridad para delimitar perímetros de seguridad, aun con carácter preventivo, cuando no constituya infracción grave.

16. Dejar sueltos o en condiciones de causar daños animales feroces o dañinos, así como abandonar animales domésticos en condiciones en que pueda peligrar su vida.

17. El consumo de bebidas alcohólicas en lugares, vías, establecimientos o transportes públicos cuando perturbe gravemente la tranquilidad ciudadana.

Artículo 38. *Prescripción de las infracciones.*

1. Las infracciones administrativas tipificadas en esta Ley prescribirán a los seis meses, al año o a los dos años de haberse cometido, según sean leves, graves o muy graves, respectivamente.

2. Los plazos señalados en esta Ley se computarán desde el día en que se haya cometido la infracción. No obstante, en los casos de infracciones continuadas y de infracciones de efectos permanentes, los plazos se computarán, respectivamente, desde el día en que se realizó la última infracción y desde que se eliminó la situación ilícita.

3. La prescripción se interrumpirá por cualquier actuación administrativa de la que tenga conocimiento formal el interesado dirigida a la sanción de la infracción, reanudándose el cómputo del plazo de prescripción si el procedimiento estuviera paralizado más de un mes por causa no imputable al presunto responsable.

4. Se interrumpirá igualmente la prescripción como consecuencia de la apertura de un procedimiento judicial penal, hasta que la autoridad judicial comunique al órgano administrativo su finalización en los términos del apartado 2 del artículo 45.

Artículo 39. *Sanciones.*

1. Las infracciones muy graves se sancionarán con multa de 30.001 a 600.000 euros; las graves, con multa de 601 a 30.000 euros, y las leves, con multa de 100 a 600 euros.

De acuerdo con lo dispuesto en el artículo 33.2, los tramos correspondientes a los grados máximo, medio y mínimo de las multas previstas por la comisión de infracciones graves y muy graves serán los siguientes:

a) Para las infracciones muy graves, el grado mínimo comprenderá la multa de 30.001 a 220.000 euros; el grado medio, de 220.001 a 410.000 euros, y el grado máximo, de 410.001 a 600.000 euros.

b) Para las infracciones graves, el grado mínimo comprenderá la multa de 601 a 10.400; el grado medio, de 10.401 a 20.200 euros, y el grado máximo, de 20.201 a 30.000 euros.

2. La multa podrá llevar aparejada alguna o algunas de las siguientes sanciones accesorias, atendiendo a la naturaleza de los hechos constitutivos de la infracción:

a) La retirada de las armas y de las licencias o permisos correspondientes a las mismas.

b) El comiso de los bienes, medios o instrumentos con los que se haya preparado o ejecutado la infracción y, en su caso, de los efectos procedentes de ésta, salvo que unos u otros pertenezcan a un tercero de buena fe no responsable de dicha infracción que los haya adquirido legalmente. Cuando los instrumentos o efectos sean de lícito comercio y su valor no guarde relación con la naturaleza o gravedad de la infracción, el órgano competente para imponer la sanción que proceda podrá no acordar el comiso o acordarlo parcialmente.

c) La suspensión temporal de las licencias, autorizaciones o permisos desde seis meses y un día a dos años por infracciones muy graves y hasta seis meses para las infracciones graves, en el ámbito de las materias reguladas en el capítulo IV de esta Ley. En caso de reincidencia, la sanción podrá ser de dos años y un día hasta seis años por infracciones muy graves y hasta dos años por infracciones graves.

d) La clausura de las fábricas, locales o establecimientos, desde seis meses y un día a dos años por infracciones muy graves y hasta seis meses por infracciones graves, en el ámbito de las materias reguladas en el capítulo IV de esta Ley. En caso de reincidencia, la sanción podrá ser de dos años y un día hasta seis años por infracciones muy graves y hasta dos años por infracciones graves.

Artículo 40. *Prescripción de las sanciones.*

1. Las sanciones impuestas por infracciones muy graves prescribirán a los tres años, las impuestas por infracciones graves, a los dos años, y las impuestas por infracciones leves al año, computados desde el día siguiente a aquel en que adquiera firmeza en vía administrativa la resolución por la que se impone la sanción.

2. Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento de ejecución, volviendo a transcurrir el plazo si aquél se paraliza durante más de un mes por causa no imputable al infractor.

Artículo 41. *Habilitación reglamentaria.*

Las disposiciones reglamentarias de desarrollo podrán introducir especificaciones o graduaciones en el cuadro de las infracciones y sanciones tipificadas en esta Ley que, sin constituir nuevas infracciones o sanciones, ni alterar su naturaleza y límites, contribuyan a la más correcta identificación de las conductas o a la más precisa determinación de las sanciones correspondientes.

Artículo 42. *Reparación del daño e indemnización.*

1. Si las conductas sancionadas hubieran ocasionado daños o perjuicios a la administración pública, la resolución del procedimiento contendrá un pronunciamiento expreso acerca de los siguientes extremos:

a) La exigencia al infractor de la reposición a su estado originario de la situación alterada por la infracción.
b) Cuando ello no fuera posible, la indemnización por los daños y perjuicios causados, si éstos hubiesen quedado determinados durante el procedimiento. Si el importe de los daños y perjuicios no hubiese quedado establecido, se determinará en un procedimiento complementario, susceptible de terminación convencional, cuya resolución pondrá fin a la vía administrativa.

2. La responsabilidad civil derivada de una infracción será siempre solidaria entre todos los causantes del daño.
3. Cuando sea declarado autor de los hechos cometidos un menor de dieciocho años no emancipado o una persona con la capacidad modificada judicialmente, responderán, solidariamente con él, de los daños y perjuicios ocasionados sus padres, tutores, curadores, acogedores o guardadores legales o de hecho, según proceda.

Artículo 43. *Registro Central de Infracciones contra la Seguridad Ciudadana.*

1. A efectos exclusivamente de apreciar la reincidencia en la comisión de infracciones tipificadas en esta Ley, se crea en el Ministerio del Interior un Registro Central de Infracciones contra la Seguridad Ciudadana.
Las comunidades autónomas que hayan asumido competencias para la protección de personas y bienes y para el mantenimiento de la seguridad ciudadana y cuenten con un cuerpo de policía propio, podrán crear sus propios registros de infracciones contra la seguridad ciudadana.
2. Reglamentariamente se regulará la organización y funcionamiento del Registro Central de Infracciones contra la Seguridad Ciudadana, en el que únicamente se practicarán los siguientes asientos:

a) Datos personales del infractor.
b) Infracción cometida.
c) Sanción o sanciones firmes en vía administrativa impuestas, con indicación de su alcance temporal, cuando proceda.
d) Lugar y fecha de la comisión de la infracción.
e) Órgano que haya impuesto la sanción.

3. Las personas a las que se haya impuesto una sanción que haya adquirido firmeza en vía administrativa serán informadas de que se procederá a la práctica de los correspondientes asientos en el Registro Central de Infracciones contra la Seguridad Ciudadana. Podrán solicitar el acceso, cancelación o rectificación de sus datos de conformidad con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y su normativa de desarrollo. Los asientos se cancelarán de oficio transcurridos tres años cuando se trate de infracciones muy graves, dos

años en el caso de infracciones graves y uno en el de infracciones leves, a contar desde la firmeza de la sanción.

4. Las autoridades y órganos de las distintas administraciones públicas con competencia sancionadora en materia de seguridad ciudadana, de acuerdo con esta Ley, comunicarán al Registro Central de Infracciones contra la Seguridad Ciudadana las resoluciones sancionadoras dictadas, una vez firmes en vía administrativa. Asimismo, a estos efectos, dichas administraciones públicas tendrán acceso a los datos obrantes en ese Registro Central.

Sección 3.ª Procedimiento sancionador

Artículo 44. *Régimen jurídico.*

El ejercicio de la potestad sancionadora en materia de protección de la seguridad ciudadana se regirá por el título IX de la Ley 30/1992, de 26 de noviembre, y sus disposiciones de desarrollo, sin perjuicio de las especialidades que se regulan en este capítulo.

Artículo 45. *Carácter subsidiario del procedimiento administrativo sancionador respecto del penal.*

1. No podrán sancionarse los hechos que hayan sido sancionados penal o administrativamente cuando se aprecie identidad de sujeto, de hecho y de fundamento.

2. En los supuestos en que las conductas pudieran ser constitutivas de delito, el órgano administrativo pasará el tanto de culpa a la autoridad judicial o al Ministerio Fiscal y se abstendrá de seguir el procedimiento sancionador mientras la autoridad judicial no dicte sentencia firme o resolución que de otro modo ponga fin al procedimiento penal, o el Ministerio Fiscal no acuerde la improcedencia de iniciar o proseguir las actuaciones en vía penal, quedando hasta entonces interrumpido el plazo de prescripción.

La autoridad judicial y el Ministerio Fiscal comunicarán al órgano administrativo la resolución o acuerdo que hubieran adoptado.

3. De no haberse estimado la existencia de ilícito penal, o en el caso de haberse dictado resolución de otro tipo que ponga fin al procedimiento penal, podrá iniciarse o proseguir el procedimiento sancionador. En todo caso, el órgano administrativo quedará vinculado por los hechos declarados probados en vía judicial.

4. Las medidas cautelares adoptadas antes de la intervención judicial podrán mantenerse mientras la autoridad judicial no resuelva otra cosa.

Artículo 46. *Acceso a los datos de otras administraciones públicas.*

1. Las autoridades y órganos de las distintas administraciones públicas competentes para imponer sanciones de acuerdo con esta Ley podrán acceder a los datos relativos a los sujetos infractores que estén directamente relacionados con la investigación de los hechos constitutivos de infracción, sin necesidad de consentimiento previo del titular de los datos, con las garantías de seguridad, integridad y disponibilidad, de conformidad con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre.

2. A los exclusivos efectos de cumplimentar las actuaciones que los órganos de la Administración General del Estado competentes en los procedimientos regulados en esta Ley y sus normas de desarrollo tienen encomendadas, la Agencia Estatal de Administración Tributaria y la Tesorería General de la Seguridad Social, en los términos establecidos en la normativa tributaria o de la seguridad social, así como el Instituto Nacional de Estadística, en lo relativo al Padrón Municipal de Habitantes, facilitarán a aquéllos el acceso a los ficheros en los que obren datos que hayan de constar en dichos procedimientos, sin que sea preciso el consentimiento de los interesados.

Artículo 47. *Medidas provisionales anteriores al procedimiento.*

1. Los agentes de la autoridad intervendrán y aprehenderán cautelarmente los instrumentos utilizados para la comisión de la infracción, así como el dinero, los frutos o los productos directamente obtenidos, que se mantendrán en los depósitos establecidos al

efecto o bajo la custodia de las Fuerzas y Cuerpos de Seguridad mientras se tramita el procedimiento sancionador o hasta que, en su caso, se resuelva la devolución o se decrete el comiso.

Sin perjuicio de lo previsto en el apartado 3 del artículo 49, si la aprehensión fuera de bienes fungibles y el coste del depósito superase el valor venal, éstos se destruirán o se les dará el destino adecuado, de acuerdo con el procedimiento que se establezca reglamentariamente.

2. Excepcionalmente, en los supuestos de grave riesgo o peligro inminente para personas o bienes, las medidas provisionales previstas en el apartado 1 del artículo 49, salvo la del párrafo f), podrán ser adoptadas directamente por los agentes de la autoridad con carácter previo a la iniciación del procedimiento, debiendo ser ratificadas, modificadas o revocadas en el acuerdo de incoación en el plazo máximo de quince días. En todo caso, estas medidas quedarán sin efecto si, transcurrido dicho plazo, no se incoa el procedimiento o el acuerdo de incoación no contiene un pronunciamiento expreso acerca de las mismas.

Artículo 48. *Actuaciones previas.*

1. Con anterioridad a la incoación del procedimiento se podrán realizar actuaciones previas con objeto de determinar si concurren circunstancias que las justifiquen. En especial, estas actuaciones se orientarán a determinar, con la mayor precisión posible, los hechos susceptibles de motivar la incoación del procedimiento, la identificación de la persona o personas que pudieran resultar responsables y las circunstancias relevantes que concurran en unos y otros.

Las actuaciones previas se incorporarán al procedimiento sancionador.

2. Las actuaciones previas podrán desarrollarse sin intervención del presunto responsable, si fuera indispensable para garantizar el buen fin de la investigación, dejando constancia escrita en las diligencias instruidas al efecto de las razones que justifican su no intervención.

3. La práctica de actuaciones previas no interrumpirá la prescripción de las infracciones.

Artículo 49. *Medidas de carácter provisional.*

1. Incoado el expediente, el órgano competente para resolver podrá adoptar en cualquier momento, mediante acuerdo motivado, las medidas de carácter provisional que resulten necesarias para asegurar la eficacia de la resolución que pudiera recaer, el buen fin del procedimiento, evitar el mantenimiento de los efectos de la infracción o preservar la seguridad ciudadana, sin que en ningún caso puedan tener carácter sancionador. Dichas medidas serán proporcionadas a la naturaleza y gravedad de la infracción y podrán consistir especialmente en:

a) El depósito en lugar seguro de los instrumentos o efectos utilizados para la comisión de las infracciones y, en particular, de las armas, explosivos, aerosoles, objetos o materias potencialmente peligrosos para la tranquilidad ciudadana, drogas tóxicas, estupefacientes o sustancias psicotrópicas.

b) La adopción de medidas de seguridad de las personas, bienes, establecimientos o instalaciones que se encuentren en situación de peligro, a cargo de sus titulares.

c) La suspensión o clausura preventiva de fábricas, locales o establecimientos susceptibles de afectar a la seguridad ciudadana.

d) La suspensión parcial o total de las actividades en los establecimientos que sean notoriamente vulnerables y no tengan en funcionamiento las medidas de seguridad necesarias.

e) La adopción de medidas de seguridad de las personas y los bienes en infraestructuras e instalaciones en las que se presten servicios básicos para la comunidad.

f) La suspensión de la actividad objeto de autorizaciones, permisos, licencias y otros documentos expedidos por las autoridades administrativas, en el marco de la normativa que le sea de aplicación.

g) La suspensión en la venta, reventa o venta ambulante de las entradas del espectáculo o actividad recreativa cuya celebración o desarrollo pudiera implicar un riesgo para la seguridad ciudadana.

2. Los gastos ocasionados por la adopción de las medidas provisionales correrán a cargo del causante de los hechos objeto del expediente sancionador.

3. La duración de las medidas de carácter provisional no podrá exceder de la mitad del plazo previsto en esta Ley para la sanción que pudiera corresponder a la infracción cometida, salvo acuerdo debidamente motivado adoptado por el órgano competente.

4. El acuerdo de adopción de medidas provisionales se notificará a los interesados en el domicilio del que tenga constancia por cualquier medio la administración o, en su caso, por medios electrónicos, con indicación de los recursos procedentes contra el mismo, órgano ante el que deban presentarse y plazos para interponerlos. La autoridad competente para su adopción podrá acordar que sea objeto de conocimiento general cuando ello sea necesario para garantizar la seguridad ciudadana, con sujeción a lo dispuesto en la legislación en materia de protección de datos de carácter personal.

5. Las medidas adoptadas serán inmediatamente ejecutivas, sin perjuicio de que los interesados puedan solicitar su suspensión justificando la apariencia de buen derecho y la existencia de daños de difícil o imposible reparación, prestando, en su caso, caución suficiente para asegurar el perjuicio que se pudiera derivar para la seguridad ciudadana.

6. Las medidas provisionales acordadas podrán ser modificadas o levantadas cuando varíen las circunstancias que motivaron su adopción y, en todo caso, se extinguirán con la resolución que ponga fin al procedimiento.

Artículo 50. *Caducidad del procedimiento.*

1. El procedimiento caducará transcurrido un año desde su incoación sin que se haya notificado la resolución, debiendo, no obstante, tenerse en cuenta en el cómputo las posibles paralizaciones por causas imputables al interesado o la suspensión que debiera acordarse por la existencia de un procedimiento judicial penal, cuando concurra identidad de sujeto, hecho y fundamento, hasta la finalización de éste.

2. La resolución que declare la caducidad se notificará al interesado y pondrá fin al procedimiento, sin perjuicio de que la administración pueda acordar la incoación de un nuevo procedimiento en tanto no haya prescrito la infracción. Los procedimientos caducados no interrumpirán el plazo de prescripción.

Artículo 51. *Efectos de la resolución.*

En el ámbito de la Administración General del Estado, la resolución del procedimiento sancionador será recurrible de conformidad con la Ley 30/1992, de 26 de noviembre. Contra la resolución que ponga fin a la vía administrativa podrá interponerse recurso contencioso-administrativo, en su caso, por el procedimiento para la protección de los derechos fundamentales de la persona, en los términos de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa.

Artículo 52. *Valor probatorio de las declaraciones de los agentes de la autoridad.*

En los procedimientos sancionadores que se instruyan en las materias objeto de esta Ley, las denuncias, atestados o actas formulados por los agentes de la autoridad en ejercicio de sus funciones que hubiesen presenciado los hechos, previa ratificación en el caso de haber sido negados por los denunciados, constituirán base suficiente para adoptar la resolución que proceda, salvo prueba en contrario y sin perjuicio de que aquéllos deban aportar al expediente todos los elementos probatorios disponibles.

Artículo 53. *Ejecución de la sanción.*

1. Una vez firme en vía administrativa, se procederá a la ejecución de la sanción conforme a lo previsto en esta Ley.

2. El cumplimiento de la sanción de suspensión de las licencias, autorizaciones o permisos se iniciará transcurrido un mes desde que la sanción haya adquirido firmeza en vía administrativa.

3. Las sanciones pecuniarias que no hayan sido abonadas previamente deberán hacerse efectivas dentro de los quince días siguientes a la fecha de la firmeza de la sanción. Una vez vencido el plazo de ingreso sin que se hubiese satisfecho la sanción, su exacción se llevará

a cabo por el procedimiento de apremio. A tal efecto, será título ejecutivo la providencia de apremio notificada al deudor, expedida por el órgano competente de la administración.

4. Cuando las sanciones hayan sido impuestas por la Administración General del Estado, los órganos y procedimientos de la recaudación ejecutiva serán los establecidos en el Reglamento General de Recaudación, aprobado por el Real Decreto 939/2005, de 29 de julio.

5. En caso de que la resolución acuerde la devolución de los instrumentos aprehendidos cautelarmente a los que se refiere el apartado 1 del artículo 47, transcurrido un mes desde la notificación de la misma sin que el titular haya recuperado el objeto aprehendido, se procederá a su destrucción o se le dará el destino adecuado en el marco de esta Ley.

Artículo 54. *Procedimiento abreviado.*

1. Una vez notificado el acuerdo de incoación del procedimiento para la sanción de infracciones graves o leves, el interesado dispondrá de un plazo de quince días para realizar el pago voluntario con reducción de la sanción de multa, o para formular las alegaciones y proponer o aportar las pruebas que estime oportunas.

Si efectúa el pago de la multa en las condiciones indicadas en el párrafo anterior, se seguirá el procedimiento sancionador abreviado, y, en caso de no hacerlo, el procedimiento sancionador ordinario.

2. El procedimiento sancionador abreviado no será de aplicación a las infracciones muy graves.

3. Una vez realizado el pago voluntario de la multa dentro del plazo de quince días contados desde el día siguiente al de su notificación, se tendrá por concluido el procedimiento sancionador con las siguientes consecuencias:

a) La reducción del 50 por ciento del importe de la sanción de multa.

b) La renuncia a formular alegaciones. En el caso de que fuesen formuladas se tendrán por no presentadas.

c) La terminación del procedimiento, sin necesidad de dictar resolución expresa, el día en que se realice el pago, siendo recurrible la sanción únicamente ante el orden jurisdiccional contencioso-administrativo.

Disposición adicional primera. *Régimen de control de precursores de drogas y explosivos.*

El sistema de otorgamiento de licencias de actividad, así como el régimen sancionador aplicable en caso de infracción de las disposiciones comunitarias e internacionales para la vigilancia del comercio de precursores de drogas y explosivos se regirá por lo dispuesto en sus legislaciones específicas.

Disposición adicional segunda. *Régimen de protección de las infraestructuras críticas.*

La protección de las infraestructuras críticas se regirá por su normativa específica y supletoriamente por esta Ley.

Disposición adicional tercera. *Comparecencia obligatoria en los procedimientos para la obtención del Documento Nacional de Identidad y el pasaporte.*

En los procedimientos administrativos de obtención del Documento Nacional de Identidad y el pasaporte será obligatoria la comparecencia del interesado ante los órganos o unidades administrativas competentes para su tramitación.

Excepcionalmente podrá eximirse de la comparecencia personal al solicitante de un pasaporte provisional en una Misión diplomática u Oficina consular española por razones justificadas de enfermedad, riesgo, lejanía u otras análogas y debidamente acreditadas que impidan o dificulten gravemente la comparecencia.

Disposición adicional cuarta. *Comunicaciones del Registro Civil.*

A efectos de dar cumplimiento a lo dispuesto en el artículo 8.3 de la Ley, el Registro Civil comunicará al Ministerio del Interior las inscripciones de resoluciones de capacidad

modificada judicialmente, los fallecimientos o las declaraciones de ausencia o fallecimiento, de acuerdo con lo dispuesto en el artículo 80 de la Ley 20/2011, de 21 de julio, del Registro Civil.

Disposición adicional quinta. *Suspensión de sanciones pecuniarias impuestas por infracciones en materia de consumo de drogas tóxicas, estupefacientes o sustancias psicotrópicas cometidas por menores de edad.*

Las multas que se impongan a los menores de edad por la comisión de infracciones en materia de consumo o tenencia ilícitos de drogas tóxicas, estupefacientes o sustancias psicotrópicas podrán suspenderse siempre que, a solicitud de los infractores y sus representantes legales, aquéllos accedan a someterse a tratamiento o rehabilitación, si lo precisan, o a actividades de reeducación. En caso de que los infractores abandonen el tratamiento o rehabilitación o las actividades reeducativas, se procederá a ejecutar la sanción económica.

Reglamentariamente se regularán los términos y condiciones de la remisión parcial de sanciones prevista en esta disposición adicional.

Disposición adicional sexta. *Infraestructuras e instalaciones en las que se prestan servicios básicos para la comunidad.*

A los efectos de lo dispuesto en los artículos 35.1 y 36.9, se entenderá por infraestructuras o instalaciones en las que se prestan servicios básicos para la comunidad:

a) Centrales nucleares, petroquímicas, refinerías y depósitos de combustible.
b) Puertos, aeropuertos y demás infraestructuras de transporte.
c) Servicios de suministro y distribución de agua, gas y electricidad.
d) Infraestructuras de telecomunicaciones.

Disposición adicional séptima. *No incremento de gasto público.*

Las medidas contempladas en esta Ley no generarán incremento de dotaciones ni de retribuciones, ni de otros gastos de personal al servicio del sector público.

Disposición transitoria única. *Procedimientos sancionadores iniciados a la entrada en vigor de esta Ley.*

Los procedimientos sancionadores iniciados a la entrada en vigor de esta Ley se regirán por la legislación anterior, salvo que esta Ley contenga disposiciones más favorables para el interesado.

Disposición derogatoria única. *Derogación normativa.*

1. Queda derogada la Ley Orgánica 1/1992, de 21 de febrero, sobre Protección de la Seguridad Ciudadana.
2. Asimismo, quedan derogadas cuantas disposiciones, de igual o inferior rango, se opongan a lo dispuesto en esta Ley.

Disposición final primera. *Régimen especial de Ceuta y Melilla.*

1. Se adiciona una disposición adicional décima a la Ley Orgánica 4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social, con la siguiente redacción:

> **«Disposición adicional décima.** *Régimen especial de Ceuta y Melilla.*
>
> 1. Los extranjeros que sean detectados en la línea fronteriza de la demarcación territorial de Ceuta o Melilla mientras intentan superar los elementos de contención fronterizos para cruzar irregularmente la frontera podrán ser rechazados a fin de impedir su entrada ilegal en España.
> 2. En todo caso, el rechazo se realizará respetando la normativa internacional de derechos humanos y de protección internacional de la que España es parte.

3. Las solicitudes de protección internacional se formalizarán en los lugares habilitados al efecto en los pasos fronterizos y se tramitarán conforme a lo establecido en la normativa en materia de protección internacional.»

Téngase en cuenta que se declara que la disposición adicional décima de la Ley Orgánica 4/2000, de 11 de enero, es conforme a la Constitución, siempre que se interprete tal y como se ha indicado en el FJ 8 C), de la Sentencia del TC 172/2020, de 19 de noviembre. Ref. BOE-A-2020-16819, concretado en los siguientes puntos:
a) Aplicación a las entradas individualizadas.
b) Pleno control judicial.
c) Cumplimiento de las obligaciones internacionales.
Asimismo, se declara que la disposición adicional décima es conforme a la Constitución, siempre que se interprete tal y como se ha indicado en el fundamento jurídico 2 e), por la Sentencia del TC 13/2021, de 28 de enero. Ref. BOE-A-2021-2832

2. La disposición final cuarta de la Ley Orgánica 4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social, queda redactada del siguiente modo:

«Disposición final cuarta. *Preceptos no orgánicos.*

1. Tienen naturaleza orgánica los preceptos contenidos en los siguientes artículos de esta Ley: 1, 2, 3, 4.1, 4.3, 5, 6, 7, 8, 9, 11, 15, 16, 17, 18, 18 bis, 19, 20, 21, 22.1, 23, 24, 25, 25 bis, 27, 29, 30, 30 bis, 31, 31 bis, 33, 34, 36, 37, 39, 40, 41, 42, 53, 54, 55, 57, 58, 59, 59 bis, 60, 61, 62, 62 bis, 62 ter, 62 quáter, 62 quinquies, 62 sexies, 63, 63 bis, 64, 66, 71, las disposiciones adicionales tercera a octava y décima y las disposiciones finales.
2. Los preceptos no incluidos en el apartado anterior no tienen naturaleza orgánica.»

Disposición final segunda. *Títulos competenciales.*

Las disposiciones de esta Ley se dictan al amparo del artículo 149.1.29.ª de la Constitución, que atribuye al Estado la competencia exclusiva en materia de seguridad pública, excepto los artículos 28 y 29, que se dictan al amparo del artículo 149.1.26.ª de la Constitución, que atribuye al Estado la competencia exclusiva en materia de régimen de producción, comercio, tenencia y uso de armas y explosivos.

Disposición final tercera. *Preceptos que tienen carácter de Ley orgánica.*

1. Tienen carácter orgánico los preceptos de esta Ley que se relacionan a continuación:

El capítulo I, excepto el artículo 5.
Los artículos 9 y 11 del capítulo II.
El capítulo III.
Del capítulo V, el apartado 3 del artículo 30; el ordinal 1 del artículo 35; los ordinales 2, 7, 8 y 23 del artículo 36, y los ordinales 1 y 4 del artículo 37.
La disposición derogatoria única.
La disposición final primera.
La disposición final tercera.

2. Los preceptos no incluidos en el apartado anterior no tienen carácter orgánico.

Disposición final cuarta. *Habilitación para el desarrollo reglamentario.*

Se habilita al Gobierno, en el ámbito de sus competencias, para dictar las disposiciones necesarias para el desarrollo y aplicación de lo establecido en esta Ley.

Disposición final quinta. *Entrada en vigor.*

Esta Ley orgánica entrará en vigor el 1 de julio de 2015, salvo la disposición final primera, que entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

§ 27

Ley 5/2014, de 4 de abril, de Seguridad Privada

Jefatura del Estado
«BOE» núm. 83, de 5 de abril de 2014
Última modificación: 27 de mayo de 2021
Referencia: BOE-A-2014-3649

JUAN CARLOS I

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley:

PREÁMBULO

I

La seguridad no es solo un valor jurídico, normativo o político; es igualmente un valor social. Es uno de los pilares primordiales de la sociedad, se encuentra en la base de la libertad y la igualdad y contribuye al desarrollo pleno de los individuos.

Los Estados, al establecer el modelo legal de seguridad privada, lo perfilan como la forma en la que los agentes privados contribuyen a la minoración de posibles riesgos asociados a su actividad industrial o mercantil, obtienen seguridad adicional más allá de la que provee la seguridad pública o satisfacen sus necesidades de información profesional con la investigación de asuntos de su legítimo interés. En esta óptica, la existencia de la seguridad privada se configura como una medida de anticipación y prevención frente a posibles riesgos, peligros o delitos. La consideración de la seguridad privada como una actividad con entidad propia, pero a la vez como parte integrante de la seguridad pública, es hoy un hecho innegable.

No solo en España sino fundamentalmente en nuestro entorno europeo, la seguridad privada se ha convertido en un verdadero actor de las políticas globales y nacionales de seguridad.

En los últimos años se han producido notables avances en la consideración ciudadana y en el replanteamiento del papel del sector privado de la seguridad, reconociéndose la importancia, eficacia y eficiencia de las alianzas público-privadas como medio para hacer frente y resolver los problemas acuciantes y variados de seguridad que se producen en la sociedad. Cada vez más, la seguridad privada se considera una parte indispensable del conjunto de medidas destinadas a la protección de la sociedad y a la defensa de los derechos y legítimos intereses de los ciudadanos.

La seguridad, entendida como pilar básico de la convivencia ejercida en régimen de monopolio por el poder público del Estado, tanto en su vertiente preventiva como investigadora, encuentra en la realización de actividades de seguridad por otras instancias sociales o agentes privados una oportunidad para verse reforzada, y una forma de articular el reconocimiento de la facultad que tienen los ciudadanos de crear o utilizar los servicios privados de seguridad con las razones profundas sobre las que se asienta el servicio público de la seguridad.

La proyección de la Administración del Estado sobre la prestación de servicios de seguridad por entidades privadas y sobre su personal se basa en el hecho de que los servicios que prestan forman parte del núcleo esencial de la competencia exclusiva en materia de seguridad pública atribuida al Estado por el artículo 149.1.29.ª de la Constitución, y en la misión que, según el artículo 104 del propio texto fundamental, incumbe a las Fuerzas y Cuerpos de Seguridad, bajo la dependencia del Gobierno, de proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana.

A partir de ahí, se establece un conjunto de controles e intervenciones administrativas que condicionan el ejercicio de las actividades de seguridad por los particulares. Ello significa que las Fuerzas y Cuerpos de Seguridad han de estar permanentemente presentes en el desarrollo de las actividades privadas de seguridad, conociendo la información trascendente para la seguridad pública que en las mismas se genera y actuando con protagonismo indiscutible, siempre que tales actividades detecten el acaecimiento de hechos delictivos o que puedan afectar a la seguridad ciudadana.

La defensa de la seguridad y el legítimo derecho a usarla no pueden ser ocasión de agresión o desconocimiento de derechos o invasión de las esferas jurídicas y patrimoniales de otras personas. Y ésta es una de las razones que justifican la intensa intervención en la organización y desarrollo de las actividades de las entidades privadas de seguridad y de su personal, por parte de la Fuerzas y Cuerpos de Seguridad, que tienen la misión constitucional de proteger los derechos fundamentales de todos los ciudadanos y garantizar su seguridad.

Desde otra perspectiva, pero igualmente integrada en el objeto de regulación de esta ley, es necesario dar el paso de reconocer la especificidad de los servicios de investigación privada el papel que han alcanzado en nuestra sociedad en los últimos años. Siendo diferentes de los demás servicios de seguridad privada, su acogida en esta norma, dentro del conjunto de actividades de seguridad privada, refleja la configuración de aquéllos como un elemento más que contribuye a garantizar la seguridad de los ciudadanos, entendida en un sentido amplio.

II

La Ley 23/1992, de 30 de julio, de Seguridad Privada, que ahora se deroga, vino a ordenar un sector hasta entonces regulado por una normativa dispersa, de rango inferior y de orientación preconstitucional en algunos casos, que contemplaba una realidad todavía incipiente, y a la que dicho marco legal permitió desarrollarse de forma armónica hasta alcanzar la importancia y transcendencia que ahora tiene, habiendo sabido concitar la generalizada aceptación de la sociedad española.

Ciertamente, la Ley 23/1992, de 30 de julio, así como su normativa de desarrollo, ha supuesto un gran avance para la evolución de la seguridad privada en España, e incluso ha constituido un modelo para procesos normativos análogos en otros Estados de la Unión Europea. Sin embargo, resulta imprescindible alumbrar una nueva normativa legal que dé solución a los problemas detectados y permita seguir evolucionando a un sector de la industria de servicios española que tanto ha contribuido a la seguridad.

En efecto, la regulación del año 1992 resulta hoy claramente insuficiente, lo que se percibe en sus profundas lagunas y carencias, paliadas parcialmente en el posterior reglamento de desarrollo, aprobado por el Real Decreto 2364/1994, de 9 de diciembre, e incluso por normas de rango inferior o simples resoluciones. Han sido en muchas ocasiones este tipo de normas las que han permitido que la Ley 23/1992, de 30 de julio, haya podido mantener su vigencia hasta el momento actual.

Además, la pertenencia de nuestro país a la Unión Europea ha obligado a que la norma fundamental que regula en España la seguridad privada, la Ley 23/1992, de 30 de junio,

haya debido ser modificada por los Reales Decretos-leyes 2/1999, de 29 de enero, y 8/2007, de 14 de septiembre, así como por la Ley 25/2009, de 22 de diciembre, de modificación de diversas Leyes para su adaptación a la Ley sobre libre acceso a las actividades de servicios y su ejercicio, con la finalidad de adaptarse cada vez a un entorno más abierto y globalizado, fenómeno que la citada ley, lógicamente, consideró de manera muy colateral.

Otros dos factores determinantes de la necesidad de sustituir la vigente ley cabecera de este sector del ordenamiento jurídico son los importantísimos cambios tecnológicos, que condicionan la prestación de servicios de seguridad, y la tendencia a la integración de las distintas seguridades en un concepto de seguridad integral, cuestión a tener en cuenta tanto en el ámbito de las actividades como en el de las funciones y servicios que presta el personal de seguridad privada, aspectos éstos que la Ley 23/1992, de 30 de julio, no podía contemplar.

Pasados veinte años desde su promulgación, ante un sector maduro y completamente profesionalizado, con presencia en todos los lugares y niveles de la vida del país y de sus ciudadanos, y ante una realidad completamente diferente a la del año 1992, es necesario aprobar una nueva norma que permita solucionar los problemas de funcionamiento detectados a lo largo de estas dos décadas pasadas.

Este fenómeno de insuficiencia de regulación se da aún más, si cabe, con las actividades de investigación privada y los detectives privados, cuya inserción tangencial en la Ley 23/1992, de 30 de julio, vino a abundar en el problema expuesto. En efecto son muy escasas las prevenciones sobre dichas actividades y personal no sólo en sede legal, sino también reglamentaria, por lo cual esta ley afronta de manera decidida y completa, en lo que le corresponde, la definición de su contenido, perfiles, limitaciones y características de quienes, convenientemente formados y habilitados, la desarrollan. De esta manera la regulación de las actividades y el personal de investigación privada pasa a constituir uno de los elementos fundamentales de la nueva ley, abandonando la presencia colateral que tiene en la vigente normativa.

III

Al contrario de la anterior regulación, la nueva ley representa un tratamiento total y sistemático de la seguridad privada en su conjunto, que pretende abarcar toda la realidad del sector existente en España, al tiempo que lo prepara para el futuro.

En consecuencia, es preciso transitar desde la concepción de control y sanción, que inspira el preámbulo y el articulado de la Ley 23/1992, de 30 de julio, y que tuvo su razón de ser en aquel momento, hasta una norma que permita aprovechar las enormes potencialidades que presenta la seguridad privada desde la perspectiva del interés público.

Es por eso que la nueva regulación contempla, entre otros objetivos, la mejora de la eficacia en la prestación de los servicios de seguridad privada en lo relativo a organización y planificación, formación y motivación del personal de seguridad; la eliminación de las situaciones que dan lugar al intrusismo tanto de las empresas como del personal; la dotación al personal de seguridad privada del respaldo jurídico necesario para el ejercicio de sus funciones legales, y los elementos de colaboración entre la seguridad privada y la seguridad pública.

La ley pasa de poner el acento en el principio de la subordinación a desarrollar más eficazmente el principio de complementariedad a través de otros que lo desarrollan, como los de cooperación o de corresponsabilidad, mediante una técnica legislativa más flexible que permite una adaptación permanente a los cambios que experimente la sociedad sin que sea precisa una reforma de rango legal para ello.

En la relación especial que mantiene la seguridad privada con las Fuerzas y Cuerpos de Seguridad, auténticos garantes del sistema de libertades y derechos que constitucionalmente protegen, se hace necesario avanzar en fórmulas jurídicas que reconozcan el papel auxiliar y especialmente colaborador desempeñado por la seguridad privada, de forma que, además de integrar funcionalmente sus capacidades en el sistema público de seguridad, les haga partícipes de la información que resulte necesaria para el mejor cumplimiento de sus deberes.

Se aborda, así, una reforma en profundidad de la regulación legal hasta ahora vigente que pivota sobre dos ejes. En primer lugar, sobre la base irrenunciable de la preeminencia

de la seguridad pública sobre la seguridad privada, se realiza una adecuación de la normativa que permita su adaptación y dé respuesta a la necesidad real de seguridad en cada momento, de manera que se aprovechen todas sus potencialidades. En segundo lugar, los poderes de intervención y control público sobre la seguridad privada se focalizan en los aspectos verdaderamente esenciales para la seguridad pública, desregulando los aspectos accesorios que no tienen una directa relación con el servicio de seguridad, al tiempo que se moderniza su gestión y se potencia su colaboración con la seguridad pública.

En resumen, puede decirse que el conjunto de los cambios propuestos en la nueva ley, además de mejorar y resolver problemas técnicos, de gestión y operativos, profundiza decididamente en el actual modelo español de seguridad privada (complementaria, subordinada, colaboradora y controlada por la seguridad pública), apostando por su papel preventivo en beneficio de la seguridad general, y lo hace aprovechando e integrando funcionalmente todo su potencial informativo, de recursos humanos y de medios materiales, al servicio de la protección y seguridad del conjunto de la ciudadanía, de forma compatible con el legítimo interés que persiguen las entidades privadas de seguridad.

Este mismo enfoque inspira los preceptos que se dedican a la investigación privada. En este punto, el legislador, como en las restantes actividades contempladas en la ley, tiene que hacer compatible ese enfoque positivo con una serie de prevenciones indispensables para garantizar los derechos de los ciudadanos, especialmente los del artículo 18 de la Constitución.

IV

Uno de los aspectos donde más se ha puesto de manifiesto el cambio habido desde la aprobación de la Ley 23/1992, de 30 de julio, es en la participación de las comunidades autónomas en la materia. Lo que entonces era algo residual se ha transformado en un fenómeno de mayor calado, pues a las comunidades autónomas con competencia estatutariamente asumida para la protección de personas y bienes y el mantenimiento del orden público, se van uniendo otras comunidades autónomas cuyos nuevos estatutos de autonomía reconocen su competencia sobre la seguridad privada, aunque en ambos casos con sujeción a lo que el Estado regule de acuerdo con el artículo 149.1.29.ª de la Constitución.

Así, la nueva ley quiere reconocer este cambio de situación y contemplar el fenómeno de una manera global, no tangencial, como hasta el momento, reflejando los diferentes niveles competenciales en función de las previsiones estatutarias.

Para que la actuación de las distintas administraciones públicas sea coherente con el mantenimiento de la armonía del sistema, es fundamental incidir en los principios de coordinación y cooperación interadministrativa.

Al objeto de evitar interferencias y duplicidades, se prevén mecanismos de coordinación institucional, se clarifica el reparto de competencias estatales y autonómicas, se afianza la competencia exclusiva del Estado en materia normativa y se sitúan en la órbita ejecutiva las competencias de las comunidades autónomas.

V

Se pasa de un tratamiento normativo parcial a una ley generalista, reguladora de la totalidad de materias que configuran el sector de la seguridad privada, dotada de sistematicidad normativa a lo largo de sus siete títulos, con un desglose de materias que abarcan desde lo más general hasta lo más específico.

Así, en el título preliminar se ha aprovechado para dar definición legal a conceptos o términos que hasta ahora permanecían jurídicamente imprecisos o indeterminados, tales como el propio de seguridad privada, o los de actividades de seguridad, servicios de seguridad, funciones de seguridad, medidas de seguridad, despachos de detectives privados u otros de significada importancia, lo que sin duda alguna ha de tener una directa repercusión favorable en la mejora de la seguridad jurídica.

En esta línea, por primera vez se fija el ámbito material y la finalidad a la que sirve la propia seguridad privada, que no puede ser otra que contribuir, con su acción profesional, a completar la seguridad pública de la que forma parte.

Otras importantes novedades que la nueva ley incorpora en su título preliminar son las referidas a la actualización del ámbito de las actividades de seguridad privada; se regulan las llamadas actividades compatibles, consistentes en todas aquellas materias que rodean o tienen incidencia directa con el mundo de la seguridad, y, por otra parte, se completan y perfilan mejor las actividades de seguridad privada, como es el caso de la investigación privada, que se incluye con normalidad en el catálogo de actividades de seguridad.

Además, se reconoce a los operadores de seguridad la condición de personal acreditado como respuesta al gran avance tecnológico y profunda transformación que ha experimentado la actividad de verificación de alarmas.

La seguridad de la información y las comunicaciones aparece por primera vez configurada no como actividad específica de seguridad privada, sino como actividad compatible que podrá ser desarrollada tanto por empresas de seguridad como por las que no lo sean, y que, por su incidencia directa en la seguridad de las entidades públicas y privadas, llevará implícito el sometimiento a ciertas obligaciones por parte de proveedores y usuarios.

Igualmente, en la línea de reducir restricciones a la libre competencia, se liberaliza la actividad de planificación, consultoría y asesoramiento en materia de seguridad privada, que pasa a considerarse como una actividad compatible no reservada a las empresas de seguridad privada, ya que su afección a esta última, y mediatamente a la seguridad pública, no es directa.

También se ha aprovechado para realizar una necesaria matización del principio general de exclusión de la seguridad privada de los espacios públicos, cuya formulación actual, excesivamente rígida, ha dificultado o impedido la necesaria autorización de servicios en beneficio del ciudadano, que resulta hoy obsoleta.

En el título I se plasma una de las ideas claves que han inspirado la redacción de la ley, como es la coordinación y la colaboración entre los servicios de seguridad privada y las Fuerzas y Cuerpos de Seguridad, con el único objetivo de mejorar la seguridad pública, mediante el intercambio de información siempre con todas las garantías legales, y la apuesta decidida por unos órganos de encuentro que han de ser mucho más proactivos que hasta el momento.

En el título II se da rango legal a algunos preceptos dedicados a la regulación de empresas de seguridad y despachos de detectives, o a los registros de ambos, que se unifican en el nuevo Registro Nacional de Seguridad Privada.

Además, se regula un sistema flexible que permitirá, cuando sea necesario por razón de las instalaciones vigiladas, aumentar los requisitos de las empresas, o reducirlos por razón de la actividad desempeñada.

En línea con el favorecimiento de la actividad económica, la ley sustituye el sistema más gravoso de la autorización administrativa por el de la declaración responsable para los centros de formación de personal de seguridad privada, los despachos de detectives privados y las empresas de instalación y mantenimiento.

En el título III se regulan cuestiones anteriormente dejadas al reglamento, donde no tenían correcta ubicación, tales como las relativas a las funciones de gran parte del personal de seguridad, ya que la Ley 23/1992, de 30 de julio, tan sólo se ocupaba de las funciones de los vigilantes de seguridad y de los detectives privados.

La ley modifica el nombre de los guardas particulares del campo, para configurarlos, más adecuadamente, como guardas rurales.

Por otra parte, se resuelve el problema del requisito de la nacionalidad española o de un Estado de la Unión Europea o de un Estado parte en el Acuerdo sobre el Espacio Económico Europeo para poder acceder a las profesiones de seguridad, que ahora se amplía a los nacionales de terceros Estados que tengan suscrito con España un convenio internacional en el que se contemple tal posibilidad a los nacionales de ambos Estados.

Otra de las novedades que se incorpora en materia de personal, largamente demandada por el sector, es la protección jurídica análoga a la de los agentes de la autoridad del personal de seguridad privada frente a las agresiones o desobediencias de que pueden ser objeto cuando desarrollen, debidamente identificados, las actividades de seguridad privada en cooperación y bajo el mando de las Fuerzas y Cuerpos de Seguridad.

Además de eliminar el inadecuado y distorsionador período de inactividad, que tantas dificultades y problemas ha supuesto para la normal reincorporación al sector del personal

de seguridad privada, en la formación del personal, junto al actual sistema de acceso a la profesión a través exclusivamente del Ministerio del Interior, se da cabida a otras posibilidades de acceso mediante el sistema que determine el Gobierno, a propuesta del Ministerio de Educación, Cultura y Deporte, al contemplarse la posibilidad de una formación profesional reglada o de grado universitario para el acceso a las diferentes profesiones de seguridad privada, o de los correspondientes certificados de profesionalidad del Ministerio de Empleo y Seguridad Social.

En el título IV se regulan por primera vez en una norma de rango legal y de forma armónica las medidas de seguridad, así como la especificación de la forma de prestación de los principales servicios de seguridad (vigilancia y protección, protección personal, depósitos y transportes de seguridad, e investigación privada), dotando de concreción a otros importantes servicios para los que la Ley 23/1992, de 30 de julio, y su reglamento de desarrollo no contienen más que referencias aisladas (verificación y respuesta ante alarmas, instalación y mantenimiento de sistemas), o no contienen regulación alguna, como sucede con la videovigilancia en el ámbito de la seguridad privada, en cumplimiento del mandato contenido en la Ley Orgánica 4/1997, de 4 de agosto, de utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos.

En este título resulta especialmente relevante la regulación de los servicios de videovigilancia y de investigación privada, ya que se trata de servicios que potencialmente pueden incidir de forma directa en la esfera de la intimidad de los ciudadanos. En el segundo caso, desde el ánimo de compaginar los diversos intereses en juego, se abordan cuestiones tan delicadas como la legitimidad del encargo, el contenido del informe de investigación o el deber de reserva profesional.

En el título V se recogen, también por vez primera en sede legal, las actuaciones de control e inspección sobre las entidades, el personal y las medidas de seguridad, así como la obligación de colaboración por parte de los afectados. Especialmente relevante es la incorporación de un precepto que regula las medidas provisionales que pueden adoptar los funcionarios policiales, cuando en el marco de una inspección lo consideren absolutamente necesario, quedando en todo caso sujetas a ratificación por la autoridad competente. Igualmente, se limita, por razón de la intimidad de los datos, el acceso al contenido de los informes de investigación privada en las inspecciones policiales a la mera constatación de su existencia, salvo que medien investigaciones policiales o judiciales o procedimientos sancionadores.

En el título VI se da solución a algunas de las principales carencias de la anterior legislación referidas al régimen sancionador. Así, se contemplan con la debida separación las infracciones que pueden ser cometidas por las entidades, el personal o los usuarios de seguridad privada, incluyendo, junto a estos últimos, a los centros de formación en la materia.

Se hace especial hincapié en la regulación de todas aquellas conductas infractoras que tengan por objeto evitar el intrusismo ya sea realizado por empresas de seguridad, por personal no habilitado, por empresas de servicios que desarrollan actividades materialmente de seguridad privada o por los propios usuarios.

A este respecto, es importante destacar el esfuerzo que se ha hecho en cuanto a la graduación de las infracciones y a los criterios para determinar la imposición de las correspondientes sanciones, con el objetivo básico de garantizar la mayor individualización de aquéllas.

Por último, en la parte final, el texto contempla aquellas disposiciones necesarias para garantizar una transición correcta desde la Ley 23/1992, de 30 de julio, a la nueva legislación, sobre todo hasta que ésta sea objeto del correspondiente desarrollo reglamentario.

TÍTULO PRELIMINAR

Disposiciones generales

CAPÍTULO I

Disposiciones comunes

Artículo 1. *Objeto.*

1. Esta ley tiene por objeto regular la realización y la prestación por personas privadas, físicas o jurídicas, de actividades y servicios de seguridad privada que, desarrollados por éstos, son contratados, voluntaria u obligatoriamente, por personas físicas o jurídicas, públicas o privadas, para la protección de personas y bienes. Igualmente regula las investigaciones privadas que se efectúen sobre aquéllas o éstos. Todas estas actividades tienen la consideración de complementarias y subordinadas respecto de la seguridad pública.

2. Asimismo, esta ley, en beneficio de la seguridad pública, establece el marco para la más eficiente coordinación de los servicios de seguridad privada con los de las Fuerzas y Cuerpos de Seguridad, de los que son complementarios.

Artículo 2. *Definiciones.*

A los efectos de esta ley se entiende por:

1. Seguridad privada: el conjunto de actividades, servicios, funciones y medidas de seguridad adoptadas, de forma voluntaria u obligatoria, por personas físicas o jurídicas, públicas o privadas, realizadas o prestados por empresas de seguridad, despachos de detectives privados y personal de seguridad privada para hacer frente a actos deliberados o riesgos accidentales, o para realizar averiguaciones sobre personas y bienes, con la finalidad de garantizar la seguridad de las personas, proteger su patrimonio y velar por el normal desarrollo de sus actividades.

2. Actividades de seguridad privada: los ámbitos de actuación material en que los prestadores de servicios de seguridad privada llevan a cabo su acción empresarial y profesional.

3. Servicios de seguridad privada: las acciones llevadas a cabo por los prestadores de servicios de seguridad privada para materializar las actividades de seguridad privada.

4. Funciones de seguridad privada: las facultades atribuidas al personal de seguridad privada.

5. Medidas de seguridad privada: las disposiciones adoptadas para el cumplimiento de los fines de prevención o protección pretendidos.

6. Prestadores de servicios de seguridad privada: las empresas de seguridad privada, los despachos de detectives y el personal habilitado para el ejercicio de funciones de seguridad privada.

7. Empresa de seguridad privada: las personas físicas o jurídicas, privadas, autorizadas o sometidas al régimen de declaración responsable, para prestar servicios de seguridad privada.

8. Personal de seguridad privada: las personas físicas que, habiendo obtenido la correspondiente habilitación, desarrollan funciones de seguridad privada.

9. Personal acreditado: profesores de centros de formación, ingenieros y técnicos que desarrollen las tareas que les asignan esta ley y operadores de seguridad.

10. Usuario de seguridad privada: las personas físicas o jurídicas que, de forma voluntaria u obligatoria, contratan servicios o adoptan medidas de seguridad privada.

11. Despachos de detectives privados: las oficinas constituidas por uno o más detectives privados que prestan servicios de investigación privada.

12. Centros de formación de aspirantes o de personal de seguridad privada: establecimientos sometidos al régimen de declaración responsable para impartir en sus locales formación al personal de seguridad privada.

13. Elemento, producto o servicio homologado: aquel que reúne las especificaciones técnicas o criterios que recoge una norma técnica al efecto.

14. Elemento, producto o servicio acreditado, certificado o verificado: aquel que lo ha sido por una entidad independiente, constituida a tal fin y reconocida por cualquier Estado miembro de la Unión Europea.

Artículo 3. *Ámbito de aplicación.*

1. Las disposiciones de esta ley son de aplicación a las empresas de seguridad privada, al personal de seguridad privada, a los despachos de detectives, a los servicios de seguridad privada, a las medidas de seguridad y a los contratos celebrados en éste ámbito.

2. Igualmente, en la medida que resulte pertinente en cada caso, se aplicarán a los establecimientos obligados a disponer de medidas de seguridad, a los usuarios de los servicios de seguridad privada, a los ingenieros y técnicos de las empresas de seguridad, a los operadores de seguridad, a los profesores de centros de formación, a las empresas prestadoras de servicios de seguridad informática, a las centrales receptoras de alarmas de uso propio y a los centros de formación de personal de seguridad privada.

3. El régimen sancionador y las medidas provisionales, así como el ejercicio de las facultades de inspección, serán también aplicables a aquellas empresas y personal que presten servicios o ejerzan funciones de seguridad privada sin estar autorizadas o haber presentado declaración responsable, o sin estar habilitados o acreditados para el ejercicio legal de los mismos.

Artículo 4. *Fines.*

La seguridad privada tiene como fines:

a) Satisfacer las necesidades legítimas de seguridad o de información de los usuarios de seguridad privada, velando por la indemnidad o privacidad de las personas o bienes cuya seguridad o investigación se le encomiende frente a posibles vulneraciones de derechos, amenazas deliberadas y riesgos accidentales o derivados de la naturaleza.

b) Contribuir a garantizar la seguridad pública, a prevenir infracciones y a aportar información a los procedimientos relacionados con sus actuaciones e investigaciones.

c) Complementar el monopolio de la seguridad que corresponde al Estado, integrando funcionalmente sus medios y capacidades como un recurso externo de la seguridad pública.

Artículo 5. *Actividades de seguridad privada.*

1. Constituyen actividades de seguridad privada las siguientes:

a) La vigilancia y protección de bienes, establecimientos, lugares y eventos, tanto públicos como privados, así como de las personas que pudieran encontrarse en los mismos.

b) El acompañamiento, defensa y protección de personas físicas determinadas, incluidas las que ostenten la condición legal de autoridad.

c) El depósito, custodia, recuento y clasificación de monedas y billetes, títulos-valores, joyas, metales preciosos, antigüedades, obras de arte u otros objetos que, por su valor económico, histórico o cultural, y expectativas que generen, puedan requerir vigilancia y protección especial.

d) El depósito y custodia de explosivos, armas, cartuchería metálica, sustancias, materias, mercancías y cualesquiera objetos que por su peligrosidad precisen de vigilancia y protección especial.

e) El transporte y distribución de los objetos a que se refieren los dos párrafos anteriores.

f) La instalación y mantenimiento de aparatos, equipos, dispositivos y sistemas de seguridad conectados a centrales receptoras de alarmas o a centros de control o de videovigilancia.

g) La explotación de centrales para la conexión, recepción, verificación y, en su caso, respuesta y transmisión de las señales de alarma, así como la monitorización de cualesquiera señales de dispositivos auxiliares para la seguridad de personas, de bienes muebles o inmuebles o de cumplimiento de medidas impuestas, y la comunicación a las Fuerzas y Cuerpos de Seguridad competentes en estos casos.

h) La investigación privada en relación a personas, hechos o delitos sólo perseguibles a instancia de parte.

2. Los servicios sobre las actividades relacionadas en los párrafos a) a g) del apartado anterior únicamente podrán prestarse por empresas de seguridad privada, sin perjuicio de las competencias de las Fuerzas y Cuerpos de Seguridad. Los despachos de detectives podrán prestar, con carácter exclusivo y excluyente, servicios sobre la actividad a la que se refiere el párrafo h) del apartado anterior.

3. Las entidades públicas o privadas podrán constituir, previa autorización del Ministerio del Interior o del órgano autonómico competente, centrales receptoras de alarmas de uso propio para la conexión, recepción, verificación y, en su caso, respuesta y transmisión de las señales de alarma que reciban de los sistemas de seguridad instalados en bienes inmuebles o muebles de su titularidad, sin que puedan dar, a través de las mismas, ningún tipo de servicio de seguridad a terceros.

Artículo 6. *Actividades compatibles.*

1. Quedan fuera del ámbito de aplicación de esta ley, sin perjuicio de la normativa específica que pudiera resultar de aplicación, especialmente en lo que se refiere a la homologación de productos, las siguientes actividades:

a) La fabricación, comercialización, venta, entrega, instalación o mantenimiento de elementos o productos de seguridad y de cerrajería de seguridad.

b) La fabricación, comercialización, venta o entrega de equipos técnicos de seguridad electrónica, así como la instalación o mantenimiento de dichos equipos siempre que no estén conectados a centrales de alarma o centros de control o de videovigilancia.

c) La conexión a centrales receptoras de alarmas de sistemas de prevención o protección contra incendios o de alarmas de tipo técnico o asistencial, o de sistemas o servicios de control o mantenimiento.

d) La planificación, consultoría y asesoramiento en materia de actividades de seguridad privada, que consistirá en la elaboración de estudios e informes de seguridad, análisis de riesgos y planes de seguridad referidos a la protección frente a todo tipo de riesgos, así como en auditorías sobre la prestación de los servicios de seguridad.

Estas actividades podrán desarrollarse por las empresas de seguridad privada.

2. Quedan también fuera del ámbito de aplicación de esta ley, a no ser que impliquen la asunción o realización de servicios o funciones de seguridad privada, y se regirán por las normas sectoriales que les sean de aplicación en cada caso, los siguientes servicios y funciones:

a) Las de información o de control en los accesos a instalaciones, comprendiendo el cuidado y custodia de las llaves, la apertura y cierre de puertas, la ayuda en el acceso de personas o vehículos, el cumplimiento de la normativa interna de los locales donde presten dicho servicio, así como la ejecución de tareas auxiliares o subordinadas de ayuda o socorro, todas ellas realizadas en las puertas o en el interior de inmuebles, locales públicos, aparcamientos, garajes, autopistas, incluyendo sus zonas de peajes, áreas de servicio, mantenimiento y descanso, por porteros, conserjes y demás personal auxiliar análogo.

b) Las tareas de recepción, comprobación de visitantes y orientación de los mismos, así como las de comprobación de entradas, documentos o carnés, en cualquier clase de edificios o inmuebles, y de cumplimiento de la normativa interna de los locales donde presten dicho servicio.

c) El control de tránsito en zonas reservadas o de circulación restringida en el interior de instalaciones en cumplimiento de la normativa interna de los mismos.

d) Las de comprobación y control del estado y funcionamiento de calderas, bienes e instalaciones en general, en cualquier clase de inmuebles, para garantizar su conservación y funcionamiento.

Estos servicios y funciones podrán prestarse o realizarse por empresas y personal de seguridad privada, siempre con carácter complementario o accesorio de las funciones de seguridad privada que se realicen y sin que en ningún caso constituyan el objeto principal del servicio que se preste.

3. El personal no habilitado que preste los servicios o funciones comprendidos en el apartado anterior, en ningún caso podrá ejercer función alguna de las reservadas al personal

de seguridad privada, ni portar ni usar armas ni medios de defensa, ni utilizar distintivos, uniformes o medios que puedan confundirse con los previstos para dicho personal.

4. Los prestadores de servicios de seguridad privada que vendan, entreguen, instalen o mantengan equipos técnicos de seguridad, no conectados a centrales receptoras de alarmas o a centros de control o de videovigilancia, quedan fuera del ámbito de aplicación de la legislación de seguridad privada.

5. Las empresas de seguridad privada que se dediquen a la instalación o mantenimiento de aparatos, dispositivos y sistemas de seguridad que no incluyan la conexión a centrales receptoras de alarmas o a centros de control o de videovigilancia, sólo están sometidas a la normativa de seguridad privada en lo que se refiere a las actividades y servicios de seguridad privada para las que se encontrasen autorizadas.

6. A las empresas, sean o no de seguridad privada, que se dediquen a las actividades de seguridad informática, entendida como el conjunto de medidas encaminadas a proteger los sistemas de información a fin de garantizar la confidencialidad, disponibilidad e integridad de la misma o del servicio que aquéllos prestan, por su incidencia directa en la seguridad de las entidades públicas y privadas, se les podrán imponer reglamentariamente requisitos específicos para garantizar la calidad de los servicios que presten.

Artículo 7. *Actividades excluidas.*

1. No están sujetas a esta ley las actuaciones de autoprotección, entendidas como el conjunto de cautelas o diligencias que se puedan adoptar o que ejecuten por sí y para sí mismos de forma directa los interesados, estrictamente dirigidas a la protección de su entorno personal o patrimonial, y cuya práctica o aplicación no conlleve contraprestación alguna ni suponga algún tipo de servicio de seguridad privada prestado a terceros.

Cuando los interesados tengan el carácter de empresas o entidades de cualquier tipo, en ningún caso utilizarán a sus empleados para el desarrollo de las funciones previstas en la presente ley, reservadas a las empresas y el personal de seguridad privada.

2. Queda fuera del ámbito de aplicación de esta ley la obtención por uno mismo de información o datos, así como la contratación de servicios de recepción, recopilación, análisis, comunicación o suministro de información libre obrante en fuentes o registros de acceso público.

Artículo 8. *Principios rectores.*

1. Los servicios y funciones de seguridad privada se prestarán con respeto a la Constitución, a lo dispuesto en esta ley, especialmente en lo referente a los principios de actuación establecidos en el artículo 30, y al resto del ordenamiento jurídico.

2. Los prestadores de servicios de seguridad privada colaborarán, en todo momento y lugar, con las Fuerzas y Cuerpos de Seguridad, con sujeción a lo que éstas puedan disponer en relación con la ejecución material de sus actividades.

3. De conformidad con lo dispuesto en la legislación de fuerzas y cuerpos de seguridad, las empresas de seguridad, los despachos de detectives y el personal de seguridad privada tendrán especial obligación de auxiliar y colaborar, en todo momento, con aquéllas en el ejercicio de sus funciones, de prestarles su colaboración y de seguir sus instrucciones, en relación con los servicios que presten que afecten a la seguridad pública o al ámbito de sus competencias.

4. Las empresas, los despachos y el personal de seguridad privada:

a) No podrán intervenir ni interferir, mientras estén ejerciendo los servicios y funciones que les son propios, en la celebración de reuniones y manifestaciones, ni en el desarrollo de conflictos políticos o laborales.

b) No podrán ejercer ningún tipo de control sobre opiniones políticas, sindicales o religiosas, o sobre la expresión de tales opiniones, ni proceder al tratamiento, automatizado o no, de datos relacionados con la ideología, afiliación sindical, religión o creencias.

c) Tendrán prohibido comunicar a terceros, salvo a las autoridades judiciales y policiales para el ejercicio de sus respectivas funciones, cualquier información que conozcan en el desarrollo de sus servicios y funciones sobre sus clientes o personas relacionadas con

éstos, así como sobre los bienes y efectos de cuya seguridad o investigación estuvieran encargados.

5. El Ministro del Interior o, en su caso, el titular del órgano autonómico competente prohibirá la utilización en los servicios de seguridad privada de determinados medios materiales o técnicos cuando pudieran causar daños o perjuicios a terceros o poner en peligro la seguridad ciudadana.

6. Cuando el personal de seguridad privada desempeñe sus funciones en entidades públicas o privadas en las que se presten servicios que resulten o se declaren esenciales por la autoridad pública competente, o en los que el servicio de seguridad se haya impuesto obligatoriamente, habrán de atenerse, en el ejercicio del derecho de huelga, a lo que respecto de dichas entidades disponga la legislación vigente.

Artículo 9. *Contratación y comunicación de servicios.*

1. No podrá prestarse ningún tipo de servicio de seguridad privada que no haya sido previamente contratado y, en su caso, autorizado.

2. De acuerdo con lo que reglamentariamente se determine, los contratos de prestación de los distintos servicios de seguridad privada deberán, en todo caso, formalizarse por escrito y comunicarse su celebración al Ministerio del Interior o, en su caso, al órgano autonómico competente con antelación a la iniciación de los mismos.

3. La comunicación de contratos de servicios de investigación privada contendrá exclusivamente los datos necesarios para identificar a las partes contratantes, excluidos los de carácter personal.

Artículo 10. *Prohibiciones.*

1. Con carácter general y además de otras prohibiciones contenidas en esta ley, se establecen las siguientes:

a) La prestación o publicidad de servicios de seguridad privada por parte de personas, físicas o jurídicas, carentes de la correspondiente autorización o sin haber presentado declaración responsable.

b) El ejercicio de funciones de seguridad privada por parte de personas físicas carentes de la correspondiente habilitación o acreditación profesional.

c) La prestación de servicios de seguridad privada incumpliendo los requisitos o condiciones legales de prestación de los mismos.

d) El empleo o utilización, en servicios de seguridad privada, de medios o medidas de seguridad no homologadas cuando sea preceptivo, o de medidas o medios personales, materiales o técnicos de forma tal que atenten contra el derecho al honor, a la intimidad personal o familiar o a la propia imagen o al secreto de las comunicaciones, o cuando incumplan las condiciones o requisitos establecidos en esta ley y en su normativa de desarrollo.

2. Los despachos de detectives y los detectives privados no podrán celebrar contratos que tengan por objeto la investigación de delitos perseguibles de oficio ni, en general, investigar delitos de esta naturaleza, debiendo denunciar inmediatamente ante la autoridad competente cualquier hecho de esta naturaleza que llegara a su conocimiento, y poniendo a su disposición toda la información y los instrumentos que pudieran haber obtenido hasta ese momento, relacionado con dichos delitos.

3. Las empresas de seguridad no podrán realizar los servicios de investigación privada propios de los despachos de detectives privados, y éstos no podrán prestar servicios propios de las empresas de seguridad privada.

Artículo 11. *Registro Nacional de Seguridad Privada y registros autonómicos.*

1. Serán objeto de inscripción de oficio en el Registro Nacional de Seguridad Privada del Ministerio del Interior, una vez concedidas las pertinentes autorizaciones o, en su caso, presentadas las declaraciones responsables, u obtenidas las preceptivas habilitaciones o acreditaciones, el personal de seguridad privada, las empresas de seguridad privada y los despachos de detectives privados, así como delegaciones y sucursales, los centros de

formación del personal de seguridad privada y las centrales receptoras de alarma de uso propio, cuando no sean objeto de inscripción en los registros de las comunidades autónomas.

Igualmente, se inscribirán en el Registro Nacional de Seguridad Privada las sanciones impuestas en materia de seguridad privada, las comunicaciones de los contratos y sus modificaciones y cuantos datos sean necesarios para las actuaciones de control y gestión de la seguridad privada, cuando tales sanciones, comunicaciones y datos se refieran a servicios de seguridad privada que se presten en un ámbito territorial distinto al de una comunidad autónoma con competencia en materia de seguridad privada.

2. En los registros de las comunidades autónomas, una vez concedidas las pertinentes autorizaciones o, en su caso, presentadas las declaraciones responsables, u obtenidas las preceptivas habilitaciones, se inscribirán de oficio las empresas de seguridad privada y los despachos de detectives privados, así como delegaciones y sucursales, los centros de formación del personal de seguridad privada y las centrales receptoras de alarma de uso propio, que tengan su domicilio en la comunidad autónoma y cuyo ámbito de actuación esté limitado a su territorio.

Igualmente, se inscribirán en dichos registros las sanciones impuestas en materia de seguridad privada, las comunicaciones de los contratos y sus modificaciones y cuantos datos sean necesarios para las actuaciones de control y gestión de la seguridad privada, cuando tales sanciones, comunicaciones y datos se refieran a servicios de seguridad privada que se presten en el ámbito territorial propio de una comunidad autónoma con competencia en materia de seguridad privada.

3. En el referido Registro Nacional, además de la información correspondiente a las empresas de seguridad privada que en el mismo se inscriban, se incorporará la relativa a las empresas de seguridad privada inscritas en los registros de las comunidades autónomas con competencia en la materia.

A tales efectos, los órganos competentes de las mencionadas comunidades autónomas deberán comunicar al Registro Nacional de Seguridad Privada los datos de las inscripciones y anotaciones que efectúen sobre las empresas de seguridad privada que inscriban, así como sus modificaciones y cancelaciones.

4. En los mencionados registros, nacional y autonómicos, se anotarán también los datos de las empresas que realicen actividades de seguridad informática, de acuerdo con lo que reglamentariamente se determine.

5. Las autoridades responsables del Registro Nacional y de los registros autonómicos establecerán los mecanismos de colaboración y reciprocidad necesarios para permitir su interconexión e interoperabilidad, la determinación coordinada de los sistemas de numeración de las empresas de seguridad privada y el acceso a la información registral contenida en los mismos, para el ejercicio de sus respectivas competencias.

6. Dichos registros serán públicos exclusivamente en cuanto a los asientos referentes a la denominación o razón social, domicilio, número de identificación fiscal y actividades en relación con las cuales estén autorizadas o hayan presentado la declaración responsable las empresas de seguridad privada, despachos de detectives, centros de formación del personal de seguridad privada y centrales de alarmas de uso propio.

7. Reglamentariamente se regulará la organización y funcionamiento del Registro Nacional de Seguridad Privada.

CAPÍTULO II

Competencias de la Administración General del Estado y de las comunidades autónomas

Artículo 12. *Competencias de la Administración General del Estado.*

1. Corresponde a la Administración General del Estado, a través del Ministerio del Interior y, en su caso, de las Delegaciones y Subdelegaciones del Gobierno, el ejercicio de las siguientes facultades:

a) La autorización o recepción de la declaración responsable, inspección y sanción de las empresas de seguridad privada y de sus delegaciones cuya competencia no haya sido asumida por las comunidades autónomas.

b) La recepción de la declaración responsable para la apertura de los despachos de detectives privados y de sus sucursales, así como su inspección y sanción, cuando el ejercicio de estas facultades no sea competencia de las comunidades autónomas.

c) La habilitación e inhabilitación del personal de seguridad privada, y la determinación del armamento, documentación, uniformidad, distintivos y medios de defensa de dicho personal, así como la acreditación, en todo caso, de los ingenieros y técnicos de las empresas de seguridad y de los operadores de seguridad.

d) La aprobación, modificación y cancelación de los programas y cursos específicos de formación del personal de seguridad privada que no sean de la competencia de los Ministerios de Educación, Cultura y Deporte o de Empleo y Seguridad Social.

e) La recepción de la declaración responsable, inspección y sanción de los centros de formación del personal de seguridad privada cuya competencia no haya sido asumida por las comunidades autónomas, así como la acreditación, en todo caso, de su profesorado.

f) La autorización, inspección y sanción de los servicios de protección personal, cuando no sea competencia de las comunidades autónomas, y de aquellas actividades y servicios transfronterizos de seguridad que puedan prestarse por las empresas y el personal de seguridad privada.

g) La autorización de los servicios de seguridad privada y de centrales de alarma de uso propio que se presten en un ámbito territorial superior al de una comunidad autónoma con competencia en materia de seguridad privada, así como la inspección y sanción de estos servicios en aquella parte de los mismos que se realice fuera del territorio de dichas comunidades autónomas.

h) La determinación reglamentaria de las características técnicas y de homologación que resulten exigibles a los productos, sistemas, dispositivos, equipos, medidas y servicios de seguridad privada.

i) La determinación reglamentaria de los establecimientos obligados a disponer de medidas de seguridad privada, así como la fijación del tipo y alcance de las medidas obligatorias que ha de cumplir cada tipo de establecimiento.

j) La autorización, inspección y sanción de los establecimientos e instalaciones industriales, comerciales y de servicios que estén obligados a adoptar medidas de seguridad, cuando el ejercicio de esas facultades no sea competencia de las comunidades autónomas.

k) La coordinación de los servicios de seguridad e investigación privadas con los de las Fuerzas y Cuerpos de Seguridad del Estado.

2. En el ámbito de las competencias de la Administración General del Estado y de conformidad con lo dispuesto en la legislación de Fuerzas y Cuerpos de Seguridad:

a) Corresponde a la Dirección General de la Policía el control de las empresas, entidades y servicios privados de seguridad, vigilancia e investigación, de su personal, medios y actuaciones.

b) Corresponde a la Dirección General de la Guardia Civil el ejercicio de sus competencias en materia de armas sobre las empresas y el personal de seguridad privada, así como el control de los guardas rurales y sus especialidades. Sin afectar a las competencias que corresponden a la Dirección General de la Policía podrá participar en el control de las actuaciones operativas del personal de seguridad privada, que preste servicios en su ámbito de competencias.

Artículo 13. *Competencias de las comunidades autónomas.*

1. Las comunidades autónomas que, con arreglo a sus estatutos de autonomía, tengan competencia para la protección de personas y bienes y para el mantenimiento del orden público, ejecutarán la legislación del Estado sobre las siguientes materias:

a) La autorización de las empresas de seguridad privada y de sus delegaciones, así como la recepción de la declaración responsable para la apertura de los despachos de

detectives privados y de sus sucursales, cuando, en ambos casos, tengan su domicilio en la comunidad autónoma y su ámbito de actuación esté limitado a su territorio.

b) La autorización de las actividades y servicios de seguridad privada que se realicen en la comunidad autónoma cuando requieran de la misma o de control previo.

c) La inspección y sanción de las actividades y servicios de seguridad privada que se realicen en la comunidad autónoma, así como de quienes los presten o utilicen y la inspección y sanción de los despachos de detectives privados y de sus sucursales que realicen su actividad en la comunidad autónoma.

d) La recepción de la declaración responsable, inspección y sanción de los centros de formación del personal de seguridad privada que tengan su sede en la comunidad autónoma.

e) La coordinación de los servicios de seguridad e investigación privadas prestados en la comunidad autónoma con los de la policía autonómica y las policías locales.

f) La autorización, inspección y sanción de los establecimientos e instalaciones industriales, comerciales y de servicios sitos en la comunidad autónoma que estén obligados a adoptar medidas de seguridad.

2. Las comunidades autónomas que, en virtud de sus estatutos de autonomía, hayan asumido competencia ejecutiva en materia de seguridad privada cuando así lo establezca la legislación del Estado, la ejercerán si disponen de cuerpo de policía propia o establecen fórmulas de colaboración con el Cuerpo Nacional de Policía previstas en la legislación de fuerzas y cuerpos de seguridad, sobre las siguientes materias:

a) La autorización, inspección y sanción de las empresas de seguridad privada que tengan su domicilio en la comunidad autónoma y cuyo ámbito de actuación esté limitado a su territorio.

b) La denuncia, y puesta en conocimiento de las autoridades competentes, de las infracciones cometidas por las empresas de seguridad que no se encuentren incluidas en el párrafo anterior.

TÍTULO I

Coordinación

Artículo 14. *Colaboración profesional.*

1. La especial obligación de colaboración de las empresas de seguridad, los despachos de detectives y el personal de seguridad privada con las Fuerzas y Cuerpos de Seguridad se desarrollará con sujeción al principio de legalidad y se basará exclusivamente en la necesidad de asegurar el buen fin de las actuaciones tendentes a preservar la seguridad pública, garantizándose la debida reserva y confidencialidad cuando sea necesario.

2. Las empresas de seguridad, los despachos de detectives y el personal de seguridad privada deberán comunicar a las Fuerzas y Cuerpos de Seguridad competentes, tan pronto como sea posible, cualesquiera circunstancias o informaciones relevantes para la prevención, el mantenimiento o restablecimiento de la seguridad ciudadana, así como todo hecho delictivo del que tuviesen conocimiento en el ejercicio de su actividad o funciones, poniendo a su disposición a los presuntos delincuentes, así como los instrumentos, efectos y pruebas relacionadas con los mismos.

3. Las Fuerzas y Cuerpos de Seguridad podrán facilitar al personal de seguridad privada, en el ejercicio de sus funciones, informaciones que faciliten su evaluación de riesgos y consiguiente implementación de medidas de protección. Si estas informaciones contuvieran datos de carácter personal sólo podrán facilitarse en caso de peligro real para la seguridad pública o para evitar la comisión de infracciones penales.

Artículo 15. *Acceso a la información por las Fuerzas y Cuerpos de Seguridad.*

1. Se autorizan las cesiones de datos que se consideren necesarias para contribuir a la salvaguarda de la seguridad ciudadana, así como el acceso por parte de las Fuerzas y Cuerpos de Seguridad a los sistemas instalados por las empresas de seguridad privada que

permitan la comprobación de las informaciones en tiempo real cuando ello sea necesario para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales.

2. El tratamiento de datos de carácter personal, así como los ficheros, automatizados o no, creados para el cumplimiento de esta ley se someterán a lo dispuesto en la normativa de protección de datos de carácter personal.

3. La comunicación de buena fe de información a las Fuerzas y Cuerpos de Seguridad por las entidades y el personal de seguridad privada no constituirá vulneración de las restricciones sobre divulgación de información impuestas por vía contractual o por cualquier disposición legal, reglamentaria o administrativa, cuando ello sea necesario para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales.

Artículo 16. *Coordinación y participación.*

1. El Ministerio del Interior o, en su caso, el órgano autonómico competente adoptará las medidas organizativas que resulten adecuadas para asegurar la coordinación de los servicios de seguridad privada con los de las Fuerzas y Cuerpos de Seguridad.

2. En el ámbito de las competencias de la Administración General del Estado se constituirán comisiones mixtas de seguridad privada, nacionales, autonómicas o provinciales, con el carácter de órganos consultivos y de colaboración entre las administraciones públicas y los representantes del sector. Su composición y funciones se determinarán reglamentariamente.

3. En las comunidades autónomas que tengan asumidas las competencias en materia de seguridad privada de conformidad con lo establecido en el artículo 13, también podrán existir órganos consultivos en materia de seguridad privada, con la composición y funcionamiento que en cada caso se determine.

TÍTULO II

Empresas de seguridad privada y despachos de detectives privados

CAPÍTULO I

Empresas de seguridad privada

Artículo 17. *Desarrollo de actividades.*

1. Las empresas de seguridad privada únicamente podrán prestar servicios sobre las actividades previstas en el artículo 5.1, excepto la contemplada en el párrafo h) del mismo.

2. Además de estas actividades, las empresas de seguridad privada podrán realizar las actividades compatibles a las que se refiere el artículo 6 y dedicarse a la formación, actualización y especialización del personal de seguridad privada, perteneciente o no a sus plantillas, en cuyo caso deberán crear centros de formación, de conformidad con lo previsto en el artículo 29.4 y a lo que reglamentariamente se determine.

3. Las empresas de seguridad privada podrán revestir forma societaria o de empresario individual, debiendo cumplir, en ambos casos, la totalidad de condiciones y requisitos previstos en este capítulo para las empresas de seguridad privada.

Artículo 18. *Autorización administrativa.*

1. Para la prestación de servicios de seguridad privada, las empresas de seguridad privada deberán obtener autorización administrativa y serán inscritas de oficio en el registro correspondiente, de acuerdo con el procedimiento que se determine reglamentariamente.

2. La autorización administrativa se suplirá por una declaración responsable cuando pretendan dedicarse exclusivamente a la actividad de seguridad privada contemplada en el artículo 5.1.f).

3. La validez de la autorización o de la declaración responsable será indefinida.

Artículo 19. *Requisitos generales.*

1. Para la autorización o, en su caso, presentación de declaración responsable, la posterior inscripción en el Registro Nacional de Seguridad Privada o en el correspondiente registro autonómico y el desarrollo de servicios de seguridad privada, las empresas de seguridad privada deberán reunir los siguientes requisitos generales:

a) Estar legalmente constituidas e inscritas en el registro mercantil o en el registro público correspondiente y tener por objeto exclusivo todas o alguna de las actividades a las que se refiere el artículo 5.1, excepto la del párrafo h). No obstante, en dicho objeto podrán incluir las actividades que resulten imprescindibles para el cumplimiento de las actividades de seguridad autorizadas, así como las compatibles contempladas en el artículo 6.

b) Tener la nacionalidad de un Estado miembro de la Unión Europea o de un Estado parte en el Acuerdo sobre el Espacio Económico Europeo.

c) Contar con los medios humanos, de formación, financieros, materiales y técnicos adecuados que, de acuerdo con el principio de proporcionalidad, se determinen reglamentariamente, en función de la naturaleza de las actividades para las que soliciten la autorización o se presente la declaración responsable, y de las características de los servicios que se prestan en relación con tales actividades. En particular, cuando se presten servicios para los que se precise el uso de armas, habrán de adoptarse las medidas que garanticen su adecuada custodia, utilización y funcionamiento. Igualmente, los ingenieros y técnicos de las empresas de seguridad privada y los operadores de seguridad, deberán disponer de la correspondiente acreditación expedida por el Ministerio del Interior, que se limitará a comprobar la honorabilidad del solicitante y la carencia de antecedentes penales, en los términos que reglamentariamente se establezca.

d) Disponer de las medidas de seguridad que reglamentariamente se determinen.

e) Suscribir un contrato de seguro de responsabilidad civil o constituir otras garantías financieras en la cuantía y con las condiciones que se determinen reglamentariamente.

f) Constituir el aval o seguro de caución que se determine reglamentariamente a disposición de las autoridades españolas, para atender exclusivamente las responsabilidades administrativas por infracciones a la normativa de seguridad privada que se deriven del funcionamiento de la empresa.

g) No haber sido condenadas mediante sentencia firme por delitos de insolvencia punible, contra la Hacienda Pública, contra la Seguridad Social, contra los derechos de los trabajadores, por intromisión ilegítima en el ámbito de protección del derecho al honor, a la intimidad personal y familiar o a la propia imagen, vulneración del secreto de las comunicaciones o de otros derechos fundamentales, salvo que hubiesen cancelado sus antecedentes penales. En el caso de las personas jurídicas, este requisito será aplicable a los administradores de hecho o de derecho y representantes, que, vigente su cargo o representación, no podrán estar incursos en la situación mencionada por actuaciones realizadas en nombre o a beneficio de dichas personas jurídicas.

h) No haber sido condenadas mediante sentencia firme por intromisión ilegítima en el ámbito de protección del derecho al honor, a la intimidad personal y familiar o a la propia imagen, vulneración del secreto de las comunicaciones o de otros derechos fundamentales en los cinco años anteriores a la solicitud. En el caso de las personas jurídicas, este requisito será aplicable a los administradores de hecho o de derecho y representantes, que, vigente su cargo o representación, no podrán estar incursos en la situación mencionada por actuaciones realizadas en nombre o a beneficio de dichas personas jurídicas.

2. Además del cumplimiento de los requisitos generales, a las empresas de seguridad privada que tengan por objeto alguna de las actividades contempladas en el artículo 5.1.b), c), d), e) y g), se les podrá exigir reglamentariamente el cumplimiento de requisitos y garantías adicionales adecuados a la singularidad de los servicios relacionados con dichas actividades.

3. Igualmente, en relación con las actividades contempladas en el artículo 5.1.a), f) y g), podrán ampliarse los requisitos referentes a medios personales y materiales, conforme se disponga reglamentariamente, para poder prestar servicios de seguridad privada en infraestructuras críticas o en servicios esenciales, así como en los servicios descritos en el artículo 40.1 y en artículo 41.2 y 3.

4. Para la contratación de servicios de seguridad privada en los sectores estratégicos definidos en la legislación de protección de infraestructuras críticas, las empresas de seguridad privada deberán contar, con carácter previo a su prestación, con una certificación emitida por una entidad de certificación acreditada que garantice, como mínimo, el cumplimiento de la normativa administrativa, laboral, de Seguridad Social y tributaria que les sea de aplicación.

5. A los efectos previstos en el apartado 1.e) y f), de este artículo se tendrán en cuenta los requisitos ya exigidos en el Estado miembro de la Unión Europea o parte en el Acuerdo sobre el Espacio Económico Europeo de origen en lo referente a la suscripción del contrato de seguro de responsabilidad civil u otras garantías financieras, así como a la constitución de avales o seguros de caución.

6. Las empresas de seguridad privada no españolas, autorizadas para la prestación de servicios de seguridad privada con arreglo a la normativa de cualquiera de los Estados miembros de la Unión Europea o de los Estados parte en el Acuerdo sobre el Espacio Económico Europeo, habrán de inscribirse obligatoriamente en el Registro Nacional de Seguridad Privada del Ministerio del Interior o, cuando tengan su domicilio en una comunidad autónoma con competencias en materia de seguridad privada y su ámbito de actuación limitado a dicho territorio, en el registro autonómico correspondiente, a cuyo efecto deberán acreditar su condición de empresas de seguridad privada y el cumplimiento de los requisitos establecidos en esta ley, en la forma que se determine reglamentariamente.

7. Sin perjuicio de lo dispuesto en los apartados anteriores, a las empresas de seguridad privada que tengan por objeto exclusivo la instalación o mantenimiento de aparatos, dispositivos y sistemas de seguridad que incluyan la prestación de servicios de conexión con centrales receptoras de alarma se las podrá eximir del cumplimiento de alguno de los requisitos incluidos en este artículo, excepto los contemplados en los párrafos e) y f) del apartado 1, cuando así se determine reglamentariamente.

8. El incumplimiento sobrevenido de los requisitos establecidos en este artículo dará lugar a la extinción de la autorización o al cierre de la empresa, en el caso de presentación de declaración responsable, y, en ambos casos, a la cancelación de oficio de la inscripción de la empresa de seguridad en el registro correspondiente.

Artículo 20. *Inscripción registral.*

1. Toda empresa de seguridad privada autorizada o que, en su caso, haya presentado la correspondiente declaración responsable será inscrita de oficio en el Registro Nacional de Seguridad Privada o en el correspondiente registro autonómico.

2. No podrá inscribirse en el Registro Nacional de Seguridad Privada o en el correspondiente registro autonómico ninguna empresa cuya denominación coincida, o pueda inducir a error o confusión, con la de otra ya inscrita o con la de órganos o dependencias de las administraciones públicas, o cuando coincida o pueda inducir a confusión con una marca anterior registrada para actividades idénticas o semejantes, salvo que se solicite por el titular de la misma o con su consentimiento.

Artículo 21. *Obligaciones generales.*

1. Las empresas de seguridad privada deberán cumplir las siguientes obligaciones generales:

a) Desarrollar las actividades de seguridad privada en los términos de esta ley y en las condiciones establecidas en la autorización que les haya sido concedida o en la declaración responsable que hayan presentado.

b) Contar con la infraestructura y logística acorde con las exigencias establecidas en esta ley y en su desarrollo reglamentario.

c) Comunicar al Registro Nacional o autonómico correspondiente todo cambio que se produzca en cuanto a su forma jurídica, denominación, número de identificación fiscal, domicilio, delegaciones, ámbito territorial de actuación, representantes legales, estatutos, titularidad de las acciones y participaciones sociales, y toda variación que sobrevenga en la composición de los órganos de administración, gestión, representación y dirección de las empresas.

Las empresas de seguridad deben comunicar al Registro Nacional o autonómico del lugar donde presten servicios las altas y bajas del personal de seguridad privada de que dispongan y las incidencias concretas relacionadas con los servicios que prestan.

d) Garantizar la formación y actualización profesional del personal de seguridad privada del que dispongan y del personal de la empresa que requiera formación en materia de seguridad privada. El mantenimiento de la aptitud en el uso de las armas de fuego se hará con la participación de instructores de tiro habilitados.

e) Presentar cada año al Ministerio del Interior o al órgano autonómico competente un informe sobre sus actividades y el resumen de las cuentas anuales, debidamente auditadas cuando sea preceptivo, con la información y datos que reglamentariamente se determinen. En ningún caso dicha memoria contendrá datos de carácter personal. El Ministerio del Interior y los órganos autonómicos competentes darán cuenta del funcionamiento del sector a las Cortes Generales y a los Parlamentos autonómicos correspondientes respectivamente, anualmente.

2. Asimismo, las empresas de seguridad privada vendrán obligadas a prestar especial auxilio y colaboración a las Fuerzas y Cuerpos de Seguridad, debiendo facilitar a éstas la información que se les requiera en relación con las competencias atribuidas a las mismas.

Artículo 22. *Representantes legales.*

1. A los efectos de esta ley, se entenderá por representante legal de las empresas de seguridad privada todo aquel que asuma o realice las tareas de dirección, administración, gestión y representación, o cualquiera de ellas, en nombre de aquéllas.

2. Los representantes de las empresas de seguridad privada, que se inscribirán en el Registro Nacional de Seguridad Privada o en el correspondiente registro autonómico, deberán:

a) Ser personas físicas residentes en el territorio de alguno de los Estados miembros de la Unión Europea o de un Estado parte en el Acuerdo sobre el Espacio Económico Europeo.

b) Carecer de antecedentes penales por delitos dolosos.

c) No haber sido sancionados en los dos o cuatro años anteriores por infracción grave o muy grave, respectivamente, en materia de seguridad privada.

d) No haber sido separados del servicio en las Fuerzas Armadas o en las Fuerzas y Cuerpos de Seguridad, ni haber ejercido funciones de control de las entidades o servicios de seguridad, vigilancia o investigación privadas, ni de su personal o medios, como miembros de las Fuerzas y Cuerpos de Seguridad, en los dos años anteriores.

e) No haber sido administrador de hecho o de derecho o apoderado general, en los diez años anteriores, en una empresa que haya sido declarada en concurso calificado como culpable, o condenada mediante sentencia firme por delitos de insolvencia punible, contra la Hacienda Pública, contra la Seguridad Social o contra los derechos de los trabajadores, por intromisión ilegítima en el ámbito de protección del derecho al honor, a la intimidad personal y familiar o a la propia imagen, vulneración del secreto de las comunicaciones o de otros derechos fundamentales.

3. Los representantes legales de las empresas de seguridad privada serán responsables del cumplimiento de las obligaciones generales impuestas a las mismas por el artículo anterior.

Artículo 23. *Consideración de sector específico.*

1. Las empresas de seguridad privada tienen la consideración de sector económico con regulación específica en materia de derecho de establecimiento.

2. Cuando el Consejo de Ministros, con arreglo a lo dispuesto en la normativa sobre inversiones extranjeras, suspenda el régimen de liberalización de los movimientos de capital, la autorización previa de inversiones de capital extranjero en empresas de seguridad privada exigirá, en todo caso, informe previo del Ministerio del Interior.

3. Las empresas de seguridad privada en las que se hubieran realizado inversiones de capital extranjero estarán obligadas a comunicar al Ministerio del Interior todo cambio que se produzca en las mismas, en relación con lo establecido en el artículo 21.1.c).

4. Las limitaciones establecidas en los dos apartados precedentes no son de aplicación a las personas físicas nacionales de los Estados miembros de la Unión Europea ni a las empresas constituidas de conformidad con la legislación de un Estado miembro y cuya sede social, administración central o centro de actividad principal se encuentre dentro de la Unión Europea.

CAPÍTULO II

Despachos de detectives privados

Artículo 24. *Apertura de despachos de detectives privados.*

1. De acuerdo con lo que se disponga reglamentariamente, podrán abrir despachos de detectives privados y, en su caso, sucursales, las personas físicas habilitadas como tales y las personas jurídicas constituidas exclusivamente por detectives privados habilitados, que únicamente podrán desarrollar la actividad mencionada en el artículo 5.1.h).

2. Los despachos de detectives privados se inscribirán de oficio en el Registro Nacional de Seguridad Privada o, en su caso, en el registro de la comunidad autónoma competente, previa presentación de declaración responsable en la forma que reglamentariamente se determine, para lo cual deberán reunir los siguientes requisitos generales:

a) Tener por objeto de su actividad profesional la realización de los servicios de investigación privada a que se refiere el artículo 48.1 y conforme a lo establecido en el artículo 10 de esta ley en materia de prohibiciones.

b) En el caso de personas jurídicas, estar legalmente constituidas e inscritas en el Registro Mercantil o en el registro público correspondiente, y cumplir con los requisitos establecidos en el artículo 19.1.g) y h).

c) Fijar un domicilio como sede física del despacho en el que se desarrollará la actividad, se llevará el libro-registro y se encontrará el archivo de los expedientes de contratación y de los informes de investigación.

d) Facilitar una relación nominal de detectives privados adscritos al despacho como integrantes asociados o dependientes del mismo.

e) Suscribir un contrato de seguro de responsabilidad civil o constituir otras garantías financieras en la cuantía y con las condiciones que se determinen reglamentariamente.

f) Constituir el aval o seguro de caución que se determine reglamentariamente a disposición de las autoridades españolas para atender exclusivamente las responsabilidades administrativas por infracciones a la normativa de seguridad privada que se deriven del funcionamiento de los despachos.

g) Mantener en todo momento el titular y los demás detectives integrantes del despacho la habilitación profesional.

h) Contar con las medidas de seguridad que reglamentariamente se determinen.

3. La validez de la declaración responsable necesaria para la apertura de los despachos de detectives y de sus sucursales será indefinida.

4. Los despachos de detectives podrán revestir forma societaria o de empresario individual, debiendo, en ambos casos, cumplir la totalidad de requisitos y obligaciones previstos en este capítulo para los despachos de detectives.

5. El incumplimiento sobrevenido de los requisitos exigidos para la apertura de los despachos de detectives producirá el cierre de los mismos y la cancelación de oficio de su inscripción en el Registro Nacional de Seguridad Privada o, en su caso, en el registro de la comunidad autónoma competente.

Artículo 25. *Obligaciones generales.*

1. Los despachos de detectives privados y sus sucursales deberán cumplir las siguientes obligaciones generales:

a) Formalizar por escrito un contrato por cada servicio de investigación que les sea encargado, comunicando su celebración al Ministerio del Interior o, en su caso, al órgano

autonómico competente en la forma que reglamentariamente se determine. Dicha obligación subsistirá igualmente en los casos de subcontratación entre despachos.

b) Llevar un libro-registro, con el formato que reglamentariamente se determine, en el que se anotará cada servicio de investigación contratado o subcontratado.

c) Informar a sus clientes sobre las incidencias relativas a los asuntos que les hubieren encargado, con entrega, en su caso, del informe de investigación elaborado.

d) Facilitar de forma inmediata a la autoridad judicial o a las Fuerzas y Cuerpos de Seguridad competentes las informaciones sobre hechos delictivos de que tuvieren conocimiento en relación con su trabajo o con las investigaciones que éstos estén llevando a cabo.

e) Acudir, cuando sean requeridos para ello por los órganos competentes de la Administración de Justicia y de las Fuerzas y Cuerpos de Seguridad, a su llamamiento, tan pronto como resulte posible, y facilitar las informaciones de que tuvieren conocimiento en relación con las investigaciones que tales organismos se encontraran llevando a cabo.

f) Atender las citaciones que realicen los juzgados y tribunales y las dependencias policiales, a los cuales sus informaciones hayan sido comunicadas o sus informes de investigación hayan sido aportados, para la prestación de testimonio y ratificación, en su caso, del contenido de los referidos informes de investigación.

g) Asegurar el archivo y conservación de la documentación relativa a su ejercicio profesional, especialmente de los contratos, informes, libros y material de imagen y sonido obtenido.

h) Comunicar al Ministerio del Interior o, en su caso, al órgano autonómico competente todo cambio que afecte a su forma jurídica, denominación, composición, domicilio y sucursales en la forma que reglamentariamente se determine.

i) Presentar al Ministerio del Interior o, en su caso, al órgano autonómico competente, una memoria anual de actividades del año precedente, con la información que se determine reglamentariamente, que no podrá contener datos de carácter personal sobre contratantes o investigados. El Ministerio del Interior y los órganos autonómicos competentes darán cuenta del funcionamiento del sector a las Cortes Generales y a los Parlamentos autonómicos correspondientes respectivamente, anualmente.

j) Depositar, en caso de cierre del despacho por cualquier causa, la documentación profesional sobre contratos, informes de investigación y libros-registros en las dependencias del Cuerpo Nacional de Policía o, en su caso, del cuerpo de policía autonómico competente.

2. Los titulares de despachos de detectives responderán civilmente de las acciones u omisiones en que, durante la ejecución de sus servicios, incurran los detectives privados dependientes o asociados.

TÍTULO III

Personal de seguridad privada

CAPÍTULO I

Disposiciones comunes

Artículo 26. *Profesiones de seguridad privada.*

1. Únicamente puede ejercer funciones de seguridad privada el personal de seguridad privada, que estará integrado por los vigilantes de seguridad y su especialidad de vigilantes de explosivos, los escoltas privados, los guardas rurales y sus especialidades de guardas de caza y guardapescas marítimos, los jefes de seguridad, los directores de seguridad y los detectives privados.

2. Para habilitarse como vigilante de explosivos será necesario haber obtenido previamente la habilitación como vigilante de seguridad.

Para habilitarse como guarda de caza o guardapesca marítimo será necesario haberlo hecho previamente como guarda rural.

3. Para la prestación de servicios en infraestructuras críticas y en aquéllos que tengan el carácter de esenciales para la comunidad, así como en aquéllos otros que excepcionalmente lo requieran en función de sus características específicas, se podrá incrementar reglamentariamente la exigencia formativa al personal de seguridad privada encargado de su realización.

4. Reglamentariamente se regulará la obtención por el personal de seguridad privada de habilitaciones adicionales a las ya adquiridas. El desarrollo reglamentario contemplará la exclusión de los requisitos de formación ya acreditados y valorará para la adquisición de dicha habilitación adicional la experiencia acreditada en el desarrollo de funciones de seguridad privada.

5. La uniformidad, distintivos y medios de defensa de los vigilantes de seguridad y de los guardas rurales y sus respectivas especialidades se determinarán reglamentariamente.

Artículo 27. *Habilitación profesional.*

1. Para el ejercicio de las funciones de seguridad privada, el personal al que se refiere el artículo anterior habrá de obtener previamente la correspondiente habilitación del Ministerio del Interior, en los términos que reglamentariamente se determinen.

2. A quienes soliciten la habilitación, previa comprobación de que reúnen los requisitos necesarios, se les expedirá la tarjeta de identidad profesional, que incluirá todas las habilitaciones de las que el titular disponga.

La tarjeta de identidad profesional constituirá el documento público de acreditación del personal de seguridad privada mientras se encuentra en el ejercicio de sus funciones profesionales.

3. La habilitación de todo el personal de seguridad privada corresponderá a la Dirección General de la Policía, excepto la de los guardas rurales y sus especialidades que corresponderá a la Dirección General de la Guardia Civil.

4. El personal de seguridad privada ejercerá exclusivamente las funciones para los que se encuentre habilitado.

5. Reglamentariamente se determinará el régimen de incompatibilidades para el ejercicio de funciones de seguridad privada.

Artículo 28. *Requisitos generales.*

1. Para la obtención de las habilitaciones profesionales indicadas en el artículo anterior, los aspirantes habrán de reunir, los siguientes requisitos generales:

a) Tener la nacionalidad de alguno de los Estados miembros de la Unión Europea o de un Estado parte en el Acuerdo sobre el Espacio Económico Europeo, o ser nacional de un tercer Estado que tenga suscrito con España un convenio internacional en el que cada parte reconozca el acceso al ejercicio de estas actividades a los nacionales de la otra.

b) Ser mayor de edad.

c) Poseer la capacidad física y la aptitud psicológica necesarias para el ejercicio de las funciones.

d) Estar en posesión de la formación previa requerida en el artículo 29.

e) Carecer de antecedentes penales por delitos dolosos.

f) No haber sido sancionado en los dos o cuatro años anteriores por infracción grave o muy grave, respectivamente, en materia de seguridad privada.

g) No haber sido separado del servicio en las Fuerzas y Cuerpos de Seguridad o en las Fuerzas Armadas españolas o del país de su nacionalidad o procedencia en los dos años anteriores.

h) No haber sido condenado por intromisión ilegítima en el ámbito de protección del derecho al honor, a la intimidad personal y familiar o a la propia imagen, vulneración del secreto de las comunicaciones o de otros derechos fundamentales en los cinco años anteriores a la solicitud.

i) Superar, en su caso, las pruebas de comprobación que reglamentariamente establezca el Ministerio del Interior, que acrediten los conocimientos y la capacidad necesarios para el ejercicio de sus funciones.

2. Además de los requisitos generales establecidos en el apartado anterior, el personal de seguridad privada habrá de reunir, para su habilitación, los requisitos específicos que reglamentariamente se determinen en atención a las funciones que haya de desempeñar.

3. La pérdida de alguno de los requisitos establecidos en este artículo producirá la extinción de la habilitación y la cancelación de oficio de la inscripción en el Registro Nacional.

4. Podrán habilitarse, pero no podrán ejercer funciones propias del personal de seguridad privada, los funcionarios públicos en activo y demás personal al servicio de cualquiera de las administraciones públicas, excepto cuando desempeñen la función de director de seguridad en el propio centro a que pertenezcan.

Los miembros de las Fuerzas y Cuerpos de Seguridad podrán ejercer funciones propias del personal de seguridad privada cuando pasen a una situación administrativa distinta a la de servicio activo, siempre que en los dos años anteriores no hayan desempeñado funciones de control de las entidades, servicios o actuaciones de seguridad, vigilancia o investigación privadas, ni de su personal o medios.

5. Los nacionales de otros Estados miembros de la Unión Europea o de Estados parte en el Acuerdo sobre el Espacio Económico Europeo, cuya habilitación o cualificación profesional haya sido obtenida en alguno de dichos Estados para el desempeño de funciones de seguridad privada en el mismo, podrán prestar servicios en España, siempre que, previa comprobación por el Ministerio del Interior, se acredite que cumplen los siguientes requisitos:

a) Poseer alguna titulación, habilitación o certificación expedida por las autoridades competentes de cualquier Estado miembro o de un Estado parte en el Acuerdo sobre el Espacio Económico Europeo que les autorice para el ejercicio de funciones de seguridad privada en el mismo.

b) Acreditar los conocimientos, formación y aptitudes equivalentes a los exigidos en España para el ejercicio de las profesiones relacionadas con la seguridad privada.

c) Tener conocimientos de lengua castellana suficientes para el normal desempeño de las funciones de seguridad privada.

d) Los previstos en los párrafos b), e), f), g) y h) del apartado 1.

6. La carencia o insuficiencia de conocimientos o aptitudes necesarios para el ejercicio en España de funciones de seguridad privada por parte de los nacionales de Estados miembros de la Unión Europea o de Estados parte en el Acuerdo sobre el Espacio Económico Europeo, podrá suplirse por aplicación de las medidas compensatorias previstas en la normativa vigente sobre reconocimiento de cualificaciones profesionales, de conformidad con lo que se determine reglamentariamente.

Artículo 29. *Formación.*

1. La formación requerida para el personal de seguridad privada consistirá:

a) Para los vigilantes de seguridad, vigilantes de explosivos, escoltas privados, guardas rurales, guardas de caza y guardapescas marítimos, en la obtención de la certificación acreditativa correspondiente, expedida por un centro de formación de personal de seguridad privada que haya presentado la declaración responsable ante el Ministerio del Interior o el órgano autonómico competente, o de los correspondientes certificados de profesionalidad de vigilancia y seguridad privada y guarderío rural y marítimo, que establezca el Gobierno a propuesta del Ministerio de Empleo y Seguridad Social, o del título de formación profesional que establezca el Gobierno a propuesta del Ministerio de Educación, Cultura y Deporte. En estos dos últimos casos no se exigirá la prueba de comprobación de conocimientos y capacidad a que se refiere el artículo 28.1.i).

b) Para los jefes y directores de seguridad, en la obtención bien de un título universitario oficial de grado en el ámbito de la seguridad que acredite la adquisición de las competencias que se determinen, o bien del título del curso de dirección de seguridad, reconocido por el Ministerio del Interior.

c) Para los detectives privados, en la obtención bien de un título universitario de grado en el ámbito de la investigación privada que acredite la adquisición de las competencias que se

determinen, o bien del título del curso de investigación privada, reconocido por el Ministerio del Interior.

2. Cuando se trate de miembros de las Fuerzas y Cuerpos de Seguridad y de las Fuerzas Armadas se tendrá en cuenta, en la forma que reglamentariamente se establezca, el grado y experiencia profesionales que acrediten su cualificación para el desempeño de las diferentes funciones de seguridad privada, siendo exigible en todo caso la prueba de comprobación de conocimientos y capacidad a que se refiere el artículo 28.1.i).

3. En relación con lo dispuesto en el apartado 1, la formación previa del personal comprendido en su párrafo a) que no posea la titulación correspondiente de formación profesional, o los certificados de profesionalidad, así como su actualización y especialización se llevará a cabo en los centros de formación de seguridad privada que hayan presentado la declaración responsable ante el Ministerio del Interior o el órgano autonómico competente. y por profesores acreditados por el citado Ministerio.

4. Los centros de formación del personal de seguridad privada requerirán, para su apertura y funcionamiento, de la presentación de la correspondiente declaración responsable ante el Ministerio del Interior u órgano autonómico competente, debiendo reunir, entre otros que reglamentariamente se establezcan, los siguientes requisitos:

a) Acreditación, por cualquier título, del derecho de uso del inmueble.
b) Licencia municipal correspondiente.
c) Relación de profesores acreditados.
d) Instalaciones adecuadas al cumplimiento de sus fines.

5. No podrán ser titulares ni desempeñar funciones de dirección ni de administración de centros de formación del personal de seguridad privada los miembros de las Fuerzas y Cuerpos de Seguridad que hayan ejercido en los mismos funciones de control de las entidades, servicios o actuaciones, o del personal o medios, en materia de seguridad privada en los dos años anteriores.

6. Las empresas de seguridad privada podrán crear centros de formación y actualización para personal de seguridad privada perteneciente o no a sus plantillas, en los términos previstos en el apartado 4.

7. El Ministerio del Interior elaborará los programas de formación previa y especializada correspondiente al personal de seguridad privada, en cuyo contenido se incluirán materias específicas de respeto a la diversidad y a la igualdad de trato y no discriminación.

Artículo 30. *Principios de actuación.*

Además de lo establecido en el artículo 8, el personal de seguridad privada se atendrá en sus actuaciones a los siguientes principios básicos:

a) Legalidad.
b) Integridad.
c) Dignidad en el ejercicio de sus funciones.
d) Corrección en el trato con los ciudadanos.
e) Congruencia, aplicando medidas de seguridad y de investigación proporcionadas y adecuadas a los riesgos.
f) Proporcionalidad en el uso de las técnicas y medios de defensa y de investigación.
g) Reserva profesional sobre los hechos que conozca en el ejercicio de sus funciones.
h) Colaboración con las Fuerzas y Cuerpos de Seguridad. El personal de seguridad privada estará obligado a auxiliar y colaborar especialmente con las Fuerzas y Cuerpos de Seguridad, a facilitarles la información que resulte necesaria para el ejercicio de sus funciones, y a seguir sus instrucciones en relación con el servicio de seguridad privada que estuvieren prestando.

Artículo 31. *Protección jurídica de agente de la autoridad.*

Se considerarán agresiones y desobediencias a agentes de la autoridad las que se cometan contra el personal de seguridad privada, debidamente identificado, cuando desarrolle actividades de seguridad privada en cooperación y bajo el mando de las Fuerzas y Cuerpos de Seguridad.

CAPÍTULO II

Funciones de seguridad privada

Artículo 32. *Vigilantes de seguridad y su especialidad.*

1. Los vigilantes de seguridad desempeñarán las siguientes funciones:

a) Ejercer la vigilancia y protección de bienes, establecimientos, lugares y eventos, tanto privados como públicos, así como la protección de las personas que puedan encontrarse en los mismos, llevando a cabo las comprobaciones, registros y prevenciones necesarias para el cumplimiento de su misión.

b) Efectuar controles de identidad, de objetos personales, paquetería, mercancías o vehículos, incluido el interior de éstos, en el acceso o en el interior de inmuebles o propiedades donde presten servicio, sin que, en ningún caso, puedan retener la documentación personal, pero sí impedir el acceso a dichos inmuebles o propiedades. La negativa a exhibir la identificación o a permitir el control de los objetos personales, de paquetería, mercancía o del vehículo facultará para impedir a los particulares el acceso o para ordenarles el abandono del inmueble o propiedad objeto de su protección.

c) Evitar la comisión de actos delictivos o infracciones administrativas en relación con el objeto de su protección, realizando las comprobaciones necesarias para prevenirlos o impedir su consumación, debiendo oponerse a los mismos e intervenir cuando presenciaren la comisión de algún tipo de infracción o fuere precisa su ayuda por razones humanitarias o de urgencia.

d) En relación con el objeto de su protección o de su actuación, detener y poner inmediatamente a disposición de las Fuerzas y Cuerpos de Seguridad competentes a los delincuentes y los instrumentos, efectos y pruebas de los delitos, así como denunciar a quienes cometan infracciones administrativas. No podrán proceder al interrogatorio de aquéllos, si bien no se considerará como tal la anotación de sus datos personales para su comunicación a las autoridades.

Lo dispuesto en el párrafo anterior se entiende sin perjuicio de los supuestos en los que la Ley de Enjuiciamiento Criminal permite a cualquier persona practicar la detención.

e) Proteger el almacenamiento, recuento, clasificación, transporte y dispensado de dinero, obras de arte y antigüedades, valores y otros objetos valiosos, así como el manipulado de efectivo y demás procesos inherentes a la ejecución de estos servicios.

f) Llevar a cabo, en relación con el funcionamiento de centrales receptoras de alarmas, la prestación de servicios de verificación personal y respuesta de las señales de alarmas que se produzcan.

Además, también podrán realizar las funciones de recepción, verificación no personal y transmisión a las Fuerzas y Cuerpos de Seguridad que el artículo 47.1 reconoce a los operadores de seguridad.

2. Los vigilantes de seguridad se dedicarán exclusivamente a las funciones de seguridad propias, no pudiendo simultanearlas con otras no directamente relacionadas con aquéllas.

3. Corresponde a los vigilantes de explosivos, que deberán estar integrados en empresas de seguridad, la función de protección del almacenamiento, transporte y demás procesos inherentes a la ejecución de estos servicios, en relación con explosivos u otros objetos o sustancias peligrosas que reglamentariamente se determinen.

Será aplicable a los vigilantes de explosivos lo establecido para los vigilantes de seguridad respecto a uniformidad, armamento y prestación del servicio.

Artículo 33. *Escoltas privados.*

1. Son funciones de los escoltas privados el acompañamiento, defensa y protección de personas determinadas, o de grupos concretos de personas, impidiendo que sean objeto de agresiones o actos delictivos.

2. En el desempeño de sus funciones, los escoltas no podrán realizar identificaciones o detenciones, ni impedir o restringir la libre circulación, salvo que resultare imprescindible como consecuencia de una agresión o de un intento manifiesto de agresión a la persona o personas protegidas o a los propios escoltas, debiendo, en tal caso, poner inmediatamente

al detenido o detenidos a disposición de las Fuerzas y Cuerpos de Seguridad, sin proceder a ninguna suerte de interrogatorio.

3. Para el cumplimiento de las indicadas funciones será aplicable a los escoltas privados lo determinado en el artículo 32 y demás preceptos concordantes, relativos a vigilantes de seguridad, salvo lo referente a la uniformidad.

Artículo 34. *Guardas rurales y sus especialidades.*

1. Los guardas rurales ejercerán funciones de vigilancia y protección de personas y bienes en fincas rústicas, así como en las instalaciones agrícolas, industriales o comerciales que se encuentren en ellas.

Se atendrán al régimen general establecido para los vigilantes de seguridad, con la especificidad de que no podrán desempeñar las funciones contempladas en el artículo 32.1.e).

2. A los guardas de caza corresponde desempeñar las funciones previstas en el apartado anterior para los guardas rurales y, además, las de vigilancia y protección en las fincas de caza en cuanto a los distintos aspectos del régimen cinegético y espacios de pesca fluvial.

3. Corresponde a los guardapescas marítimos desempeñar las funciones previstas en el apartado 1 para los guardas rurales y, además, las de vigilancia y protección de los establecimientos de acuicultura y zonas marítimas con fines pesqueros.

4. Los guardas de caza y los guardapescas marítimos podrán proceder a la retirada u ocupación de las piezas cobradas y los medios de caza y pesca, incluidas armas, cuando aquéllos hubieran sido utilizados para cometer una infracción, procediendo a su entrega inmediata a las Fuerzas y Cuerpos de Seguridad competentes.

Artículo 35. *Jefes de seguridad.*

1. En el ámbito de la empresa de seguridad en cuya plantilla están integrados, corresponde a los jefes de seguridad el ejercicio de las siguientes funciones:

a) El análisis de situaciones de riesgo y la planificación y programación de las actuaciones precisas para la implantación y realización de los servicios de seguridad privada.

b) La organización, dirección e inspección del personal y servicios de seguridad privada.

c) La propuesta de los sistemas de seguridad que resulten pertinentes, y el control de su funcionamiento y mantenimiento, pudiendo validarlos provisionalmente hasta tanto se produzca la inspección y autorización, en su caso, por parte de la Administración.

d) El control de la formación permanente del personal de seguridad que de ellos dependa, y la propuesta de la adopción de las medidas o iniciativas adecuadas para el cumplimiento de dicha finalidad.

e) La coordinación de los distintos servicios de seguridad que de ellos dependan, con actuaciones propias de protección civil en situaciones de emergencia, catástrofe o calamidad pública.

f) La garantía de la colaboración de los servicios de seguridad con los de las correspondientes dependencias de las Fuerzas y Cuerpos de Seguridad.

g) La supervisión de la observancia de la normativa de seguridad privada aplicable.

h) La responsabilidad sobre la custodia y el traslado de armas de titularidad de la empresa a la que pertenezca, de acuerdo con la normativa de armas y con lo que reglamentariamente se determine.

2. La existencia del jefe de seguridad en las empresas de seguridad privada será obligatoria siempre que éstas se dediquen a todas o algunas de las actividades previstas en los párrafos a), b), c), d) y e) del artículo 5.1.

En función de la complejidad organizativa o técnica, u otras circunstancias que se determinen reglamentariamente, podrá exigirse la existencia de un jefe de seguridad específico para algunas de dichas actividades de seguridad.

3. El ejercicio de funciones podrá delegarse por los jefes de seguridad en los términos que reglamentariamente se dispongan.

Artículo 36. *Directores de seguridad.*

1. En relación con la empresa o entidad en la que presten sus servicios, corresponde a los directores de seguridad el ejercicio de las siguientes funciones:

a) La organización, dirección, inspección y administración de los servicios y recursos de seguridad privada disponibles.
b) La identificación, análisis y evaluación de situaciones de riesgo que puedan afectar a la vida e integridad de las personas y al patrimonio.
c) La planificación, organización y control de las actuaciones precisas para la implantación de las medidas conducentes a prevenir, proteger y reducir la manifestación de riesgos de cualquier naturaleza con medios y medidas precisas, mediante la elaboración y desarrollo de los planes de seguridad aplicables.
d) El control del funcionamiento y mantenimiento de los sistemas de seguridad privada.
e) La validación provisional, hasta la comprobación, en su caso, por parte de la Administración, de las medidas de seguridad en lo referente a su adecuación a la normativa de seguridad privada.
f) La comprobación de que los sistemas de seguridad privada instalados y las empresas de seguridad privada contratadas, cumplen con las exigencias de homologación de los organismos competentes.
g) La comunicación a las Fuerzas y Cuerpos de Seguridad competentes de las circunstancias o informaciones relevantes para la seguridad ciudadana, así como de los hechos delictivos de los que tenga conocimiento en el ejercicio de sus funciones.
h) La interlocución y enlace con la Administración, especialmente con las Fuerzas y Cuerpos de Seguridad, respecto de la función de seguridad integral de la entidad, empresa o grupo empresarial que les tenga contratados, en relación con el cumplimiento normativo sobre gestión de todo tipo de riesgos.
i) Las comprobaciones de los aspectos necesarios sobre el personal que, por el ejercicio de las funciones encomendadas, precise acceder a áreas o informaciones, para garantizar la protección efectiva de su entidad, empresa o grupo empresarial.

2. Los usuarios de seguridad privada situarán al frente de la seguridad integral de la entidad, empresa o grupo empresarial a un director de seguridad cuando así lo exija la normativa de desarrollo de esta ley por la dimensión de su servicio de seguridad; cuando se acuerde por decisión gubernativa, en atención a las medidas de seguridad y al grado de concentración de riesgo, o cuando lo prevea una disposición especial.
Lo dispuesto en este apartado es igualmente aplicable a las empresas de seguridad privada.
3. En las empresas de seguridad el director de seguridad podrá compatibilizar sus funciones con las de jefe de seguridad.
4. Cuando una empresa de seguridad preste servicio a un usuario que cuente con su propio director de seguridad, las funciones encomendadas a los jefes de seguridad en el artículo 35.1.a), b), c), y e) serán asumidas por dicho director de seguridad.
5. El ejercicio de funciones podrá delegarse por los directores de seguridad en los términos que reglamentariamente se disponga.

Artículo 37. *Detectives privados.*

1. Los detectives privados se encargarán de la ejecución personal de los servicios de investigación privada a los que se refiere el artículo 48, mediante la realización de averiguaciones en relación con personas, hechos y conductas privadas.
2. En el ejercicio de sus funciones, los detectives privados vendrán obligados a:

a) Confeccionar los informes de investigación relativos a los asuntos que tuvieren encargados.
b) Asegurar la necesaria colaboración con las Fuerzas y Cuerpos de Seguridad cuando sus actuaciones profesionales se encuentren relacionadas con hechos delictivos o que puedan afectar a la seguridad ciudadana.
c) Ratificar el contenido de sus informes de investigación ante las autoridades judiciales o policiales cuando fueren requeridos para ello.

3. El ejercicio de las funciones correspondientes a los detectives privados no será compatible con las funciones del resto del personal de seguridad privada, ni con funciones propias del personal al servicio de cualquier Administración Pública.

4. Los detectives privados no podrán investigar delitos perseguibles de oficio, debiendo denunciar inmediatamente ante la autoridad competente cualquier hecho de esta naturaleza que llegara a su conocimiento, y poniendo a su disposición toda la información y los instrumentos que pudieran haber obtenido hasta ese momento.

TÍTULO IV

Servicios y medidas de seguridad

CAPÍTULO I

Disposiciones comunes

Artículo 38. *Prestación de los servicios de seguridad privada.*

1. Los servicios de seguridad privada se prestarán de conformidad con lo dispuesto en esta ley, en particular en sus artículos 8 y 30, y en sus normas de desarrollo, con arreglo a las estipulaciones del contrato, así como, en su caso, con la autorización concedida o declaración responsable presentada.

2. Los servicios de seguridad privada se prestarán únicamente por empresas de seguridad privada, despachos de detectives y personal de seguridad privada.

3. Reglamentariamente se establecerán las condiciones y requisitos para la subcontratación de servicios de seguridad privada.

4. Los vigilantes de seguridad, vigilantes de explosivos, escoltas privados y jefes de seguridad desempeñarán sus funciones profesionales integrados en las empresas de seguridad que les tengan contratados.

5. Los directores de seguridad de las empresas de seguridad privada y de las entidades obligadas a disponer de esta figura, conforme a lo dispuesto en el artículo 36, desempeñarán sus funciones integrados en las plantillas de dichas empresas.

6. Los guardas rurales podrán desarrollar sus funciones sin necesidad de constituir o estar integrados en empresas de seguridad, prestando sus servicios directamente a los titulares de bienes y derechos que les puedan contratar, conforme a lo que se establezca reglamentariamente, cuando se trate de servicios de vigilancia y protección de explotaciones agrícolas, fincas de caza, en cuanto a los distintos aspectos del régimen cinegético, y zonas marítimas protegidas con fines pesqueros.

7. Los detectives privados ejercerán sus funciones profesionales a través de los despachos de detectives para los que presten sus servicios.

Artículo 39. *Forma de prestación.*

1. Los medios utilizados por las empresas de seguridad en la prestación de los servicios de seguridad privada deberán estar homologados por el Ministerio del Interior. En todo caso, los vehículos, uniformes y distintivos no podrán inducir a confusión con los de las Fuerzas y Cuerpos de Seguridad, ni con los de las Fuerzas Armadas, y se ajustarán a las características que reglamentariamente se determinen.

2. El personal de seguridad privada uniformado, constituido por los vigilantes de seguridad y de explosivos y por los guardas rurales y sus especialidades, prestará sus servicios vistiendo el uniforme y ostentando el distintivo del cargo, y portando los medios de defensa reglamentarios, que no incluirán armas de fuego.

Reglamentariamente se podrán establecer excepciones a la obligación de desarrollar sus funciones con uniforme y distintivo.

3. Previo el otorgamiento de las correspondientes licencias, sólo se desarrollarán con armas de fuego los servicios de seguridad privada contemplados en el artículo 40 y los que reglamentariamente se determinen.

Las armas adecuadas para realizar los servicios de seguridad sólo se podrán portar estando de servicio, con las salvedades que se establezcan reglamentariamente.

4. Salvo en los casos expresamente previstos en esta ley y lo que se determine reglamentariamente atendiendo a las especiales características de determinados servicios de seguridad privada, los vigilantes de seguridad ejercerán sus funciones en el interior de los inmuebles o de las propiedades de cuya vigilancia estuvieran encargados.

5. El personal de seguridad privada, durante la prestación de los servicios de seguridad privada, portará la tarjeta de identidad profesional y, en su caso, la documentación correspondiente al arma de fuego.

CAPÍTULO II

Servicios de las empresas de seguridad privada

Artículo 40. *Servicios con armas de fuego.*

1. Los siguientes servicios de seguridad privada se prestarán con armas de fuego en los términos que reglamentariamente se determinen:

a) Los de vigilancia y protección del almacenamiento, recuento, clasificación y transporte de dinero, valores y objetos valiosos.

b) Los de vigilancia y protección de fábricas y depósitos o transporte de armas, cartuchería metálica y explosivos.

c) Los de vigilancia y protección en buques mercantes y buques pesqueros que naveguen bajo bandera española en aguas en las que exista grave riesgo para la seguridad de las personas o de los bienes.

d) Cuando por sus características y circunstancias lo requieran, los de vigilancia y protección perimetral en centros penitenciarios, centros de internamiento de extranjeros, establecimientos militares u otros edificios o instalaciones de organismos públicos, incluidas las infraestructuras críticas.

2. Reglamentariamente se determinarán aquellos supuestos en los que, valoradas circunstancias tales como localización, valor de los objetos a proteger, concentración del riesgo, peligrosidad, nocturnidad, zonas rústicas o cinegéticas, u otras de análoga significación, podrá autorizarse la prestación de los servicios de seguridad privada portando armas de fuego.

Asimismo, podrá autorizarse la prestación de los servicios de verificación personal de alarmas portando armas de fuego, cuando sea necesario para garantizar la seguridad del personal que los presta, atendiendo a la naturaleza de dicho servicio, al objeto de la protección o a otras circunstancias que incidan en aquélla.

3. El personal de seguridad privada sólo podrá portar el arma de fuego cuando esté de servicio, y podrá acceder con ella al lugar donde se desarrolle éste, salvo que legalmente se establezca lo contrario. Reglamentariamente podrán establecerse excepciones para supuestos determinados.

4. Las armas de fuego adecuadas para realizar cada tipo de servicio serán las que reglamentariamente se establezcan.

Artículo 41. *Servicios de vigilancia y protección.*

1. Los servicios de vigilancia y protección referidos a las actividades contempladas en el artículo 5.1.a) se prestarán por vigilantes de seguridad o, en su caso, por guardas rurales, que desempeñarán sus funciones, con carácter general, en el interior de los edificios, de las instalaciones o propiedades a proteger. No obstante, podrán prestarse fuera de estos espacios sin necesidad de autorización previa, incluso en vías o espacios públicos o de uso común, en los siguientes supuestos:

a) La vigilancia y protección sobre acciones de manipulación o utilización de bienes, maquinaria o equipos valiosos que hayan de tener lugar en las vías o espacios públicos o de uso común.

b) La retirada y reposición de fondos en cajeros automáticos, así como la prestación de servicios de vigilancia y protección de los mismos durante las citadas operaciones, o en las de reparación de averías.

c) Los desplazamientos al exterior de los inmuebles objeto de protección para la realización de actividades directamente relacionadas con las funciones de vigilancia y seguridad de dichos inmuebles.

d) La vigilancia y protección de los medios de transporte y de sus infraestructuras.

e) Los servicios de ronda o de vigilancia discontinua, consistentes en la visita intermitente y programada a los diferentes puestos de vigilancia establecidos o a los distintos lugares objeto de protección.

f) La persecución de quienes sean sorprendidos en flagrante delito, en relación con las personas o bienes objeto de su vigilancia y protección.

g) Las situaciones en que ello viniera exigido por razones humanitarias.

h) Los servicios de vigilancia y protección a los que se refieren los apartados siguientes.

2. Requerirán autorización previa por parte del órgano competente los siguientes servicios de vigilancia y protección, que se prestarán en coordinación, cuando proceda, con las Fuerzas y Cuerpos de Seguridad, y de acuerdo con sus instrucciones:

a) La vigilancia en polígonos industriales y urbanizaciones delimitados, incluidas sus vías o espacios de uso común.

b) La vigilancia en complejos o parques comerciales y de ocio que se encuentren delimitados.

c) La vigilancia en acontecimientos culturales, deportivos o cualquier otro evento de relevancia social que se desarrolle en vías o espacios públicos o de uso común, en coordinación, en todo caso, con las Fuerzas y Cuerpos de Seguridad.

d) La vigilancia y protección en recintos y espacios abiertos que se encuentren delimitados.

Reglamentariamente se establecerán las condiciones y requisitos para la prestación de estos servicios.

3. Cuando así se decida por el órgano competente, y cumpliendo estrictamente las órdenes e instrucciones de las Fuerzas y Cuerpos de Seguridad, podrán prestarse los siguientes servicios de vigilancia y protección:

a) La vigilancia perimetral de centros penitenciarios.

b) La vigilancia perimetral de centros de internamiento de extranjeros.

c) La vigilancia de otros edificios o instalaciones de organismos públicos.

d) La participación en la prestación de servicios encomendados a la seguridad pública, complementando la acción policial. La prestación de estos servicios también podrá realizarse por guardas rurales.

Artículo 42. *Servicios de videovigilancia.*

1. Los servicios de videovigilancia consisten en el ejercicio de la vigilancia a través de sistemas de cámaras o videocámaras, fijas o móviles, capaces de captar y grabar imágenes y sonidos, incluido cualquier medio técnico o sistema que permita los mismos tratamientos que éstas.

Cuando la finalidad de estos servicios sea prevenir infracciones y evitar daños a las personas o bienes objeto de protección o impedir accesos no autorizados, serán prestados necesariamente por vigilantes de seguridad o, en su caso, por guardas rurales.

No tendrán la consideración de servicio de videovigilancia la utilización de cámaras o videocámaras cuyo objeto principal sea la comprobación del estado de instalaciones o bienes, el control de accesos a aparcamientos y garajes, o las actividades que se desarrollan desde los centros de control y otros puntos, zonas o áreas de las autopistas de peaje. Estas funciones podrán realizarse por personal distinto del de seguridad privada.

2. No se podrán utilizar cámaras o videocámaras con fines de seguridad privada para tomar imágenes y sonidos de vías y espacios públicos o de acceso público salvo en los supuestos y en los términos y condiciones previstos en su normativa específica, previa

autorización administrativa por el órgano competente en cada caso. Su utilización en el interior de los domicilios requerirá el consentimiento del titular.

3. Las cámaras de videovigilancia que formen parte de medidas de seguridad obligatorias o de sistemas de recepción, verificación y, en su caso, respuesta y transmisión de alarmas, no requerirán autorización administrativa para su instalación, empleo o utilización.

4. Las grabaciones realizadas por los sistemas de videovigilancia no podrán destinarse a un uso distinto del de su finalidad. Cuando las mismas se encuentren relacionadas con hechos delictivos o que afecten a la seguridad ciudadana, se aportarán, de propia iniciativa o a su requerimiento, a las Fuerzas y Cuerpos de Seguridad competentes, respetando los criterios de conservación y custodia de las mismas para su válida aportación como evidencia o prueba en investigaciones policiales o judiciales.

5. La monitorización, grabación, tratamiento y registro de imágenes y sonidos por parte de los sistemas de videovigilancia estará sometida a lo previsto en la normativa en materia de protección de datos de carácter personal, y especialmente a los principios de proporcionalidad, idoneidad e intervención mínima.

6. En lo no previsto en la presente ley y en sus normas de desarrollo, se aplicará lo dispuesto en la normativa sobre videovigilancia por parte de las Fuerzas y Cuerpos de Seguridad.

Artículo 43. *Servicios de protección personal.*

1. Los servicios de protección personal, a cargo de escoltas privados, consistirán en el acompañamiento, custodia, resguardo, defensa y protección de la libertad, vida e integridad física de personas o grupos de personas determinadas.

2. La prestación de servicios de protección personal se realizará con independencia del lugar donde se encuentre la persona protegida, incluido su tránsito o circulación por las vías públicas, sin que se puedan realizar identificaciones, restricciones de la circulación, o detenciones, salvo en caso de flagrante delito relacionado con el objeto de su protección.

3. La prestación de estos servicios sólo podrá realizarse previa autorización del Ministerio del Interior o del órgano autonómico competente, conforme se disponga reglamentariamente.

Artículo 44. *Servicios de depósito de seguridad.*

1. Los servicios de depósito de seguridad, referidos a la actividad contemplada en el artículo 5.1.c), estarán a cargo de vigilantes de seguridad y se prestarán obligatoriamente cuando los objetos en cuestión alcancen las cuantías que reglamentariamente se establezcan, así como cuando las autoridades competentes lo determinen en atención a los antecedentes y circunstancias relacionadas con dichos objetos.

2. Los servicios de depósito de seguridad referidos a la actividad contemplada en el artículo 5.1.d), estarán a cargo de vigilantes de explosivos y se prestarán obligatoriamente cuando precisen de vigilancia, cuidado y protección especial, de acuerdo con la normativa específica de cada materia o así lo dispongan las autoridades competentes en atención a los antecedentes y circunstancias relacionadas con dichos objetos o sustancias.

Artículo 45. *Servicios de transporte de seguridad.*

Los servicios de transporte y distribución de los objetos y sustancias a que se refiere el artículo anterior, se llevarán a cabo mediante vehículos acondicionados especialmente para cada tipo de transporte u otros elementos de seguridad específicos homologados para el transporte, y consistirán en su traslado material y su protección durante el mismo, por vigilantes de seguridad o vigilantes de explosivos, respectivamente, con arreglo a lo prevenido en esta ley y en sus normas reglamentarias de desarrollo.

Artículo 46. *Servicios de instalación y mantenimiento.*

1. Los servicios de instalación y mantenimiento de aparatos, equipos, dispositivos y sistemas de seguridad conectados a centrales receptoras de alarmas, centros de control o de videovigilancia, consistirán en la ejecución, por técnicos acreditados, de todas aquellas

operaciones de instalación y mantenimiento de dichos aparatos, equipos, dispositivos o sistemas, que resulten necesarias para su correcto funcionamiento y el buen cumplimiento de su finalidad, previa elaboración, por ingenieros acreditados, del preceptivo proyecto de instalación, cuyas características se determinarán reglamentariamente.

2. Estos sistemas deberán someterse a revisiones preventivas con la periodicidad y forma que se determine reglamentariamente.

Artículo 47. *Servicios de gestión de alarmas.*

1. Los servicios de gestión de alarmas, a cargo de operadores de seguridad, consistirán en la recepción, verificación no personal y, en su caso, transmisión de las señales de alarma, relativas a la seguridad y protección de personas y bienes a las Fuerzas y Cuerpos de Seguridad competentes.

2. Los servicios de respuesta ante alarmas se prestarán por vigilantes de seguridad o, en su caso, por guardas rurales, y podrán comprender los siguientes servicios:

a) El depósito y custodia de las llaves de los inmuebles u objetos donde estén instalados los sistemas de seguridad conectados a la central de alarmas y, en su caso, su traslado hasta el lugar del que procediere la señal de alarma verificada o bien la apertura a distancia controlada desde la central de alarmas.

b) El desplazamiento de los vigilantes de seguridad o guardas rurales a fin de proceder a la verificación personal de la alarma recibida.

c) Facilitar el acceso a los servicios policiales o de emergencia cuando las circunstancias lo requieran, bien mediante aperturas remotas controladas desde la central de alarmas o con los medios y dispositivos de acceso de que se disponga.

3. Cuando los servicios se refirieran al análisis y monitorización de eventos de seguridad de la información y las comunicaciones, estarán sujetos a las especificaciones que reglamentariamente se determinen. Las señales de alarma referidas a estos eventos deberán ser puestas, cuando corresponda, en conocimiento del órgano competente, por el propio usuario o por la empresa con la que haya contratado la seguridad.

CAPÍTULO III

Servicios de los despachos de detectives privados

Artículo 48. *Servicios de investigación privada.*

1. Los servicios de investigación privada, a cargo de detectives privados, consistirán en la realización de las averiguaciones que resulten necesarias para la obtención y aportación, por cuenta de terceros legitimados, de información y pruebas sobre conductas o hechos privados relacionados con los siguientes aspectos:

a) Los relativos al ámbito económico, laboral, mercantil, financiero y, en general, a la vida personal, familiar o social, exceptuada la que se desarrolle en los domicilios o lugares reservados.

b) La obtención de información tendente a garantizar el normal desarrollo de las actividades que tengan lugar en ferias, hoteles, exposiciones, espectáculos, certámenes, convenciones, grandes superficies comerciales, locales públicos de gran concurrencia o ámbitos análogos.

c) La realización de averiguaciones y la obtención de información y pruebas relativas a delitos sólo perseguibles a instancia de parte por encargo de los sujetos legitimados en el proceso penal.

2. La aceptación del encargo de estos servicios por los despachos de detectives privados requerirá, en todo caso, la acreditación, por el solicitante de los mismos, del interés legítimo alegado, de lo que se dejará constancia en el expediente de contratación e investigación que se abra.

3. En ningún caso se podrá investigar la vida íntima de las personas que transcurra en sus domicilios u otros lugares reservados, ni podrán utilizarse en este tipo de servicios medios personales, materiales o técnicos de tal forma que atenten contra el derecho al

honor, a la intimidad personal o familiar o a la propia imagen o al secreto de las comunicaciones o a la protección de datos.

4. En la prestación de los servicios de investigación, los detectives privados no podrán utilizar o hacer uso de medios, vehículos o distintivos que puedan confundirse con los de las Fuerzas y Cuerpos de Seguridad.

5. En todo caso, los despachos de detectives y los detectives privados encargados de las investigaciones velarán por los derechos de sus clientes con respeto a los de los sujetos investigados.

6. Los servicios de investigación privada se ejecutarán con respeto a los principios de razonabilidad, necesidad, idoneidad y proporcionalidad.

Artículo 49. *Informes de investigación.*

1. Por cada servicio que les sea contratado, los despachos o los detectives privados encargados del asunto deberán elaborar un único informe en el que reflejarán el número de registro asignado al servicio, los datos de la persona que encarga y contrata el servicio, el objeto de la contratación, los medios, los resultados, los detectives intervinientes y las actuaciones realizadas, en las condiciones y plazos que reglamentariamente se establezcan.

2. En el informe de investigación únicamente se hará constar información directamente relacionada con el objeto y finalidad de la investigación contratada, sin incluir en él referencias, informaciones o datos que hayan podido averiguarse relativos al cliente o al sujeto investigado, en particular los de carácter personal especialmente protegidos, que no resulten necesarios o que no guarden directa relación con dicho objeto y finalidad ni con el interés legítimo alegado para la contratación.

3. Dicho informe estará a disposición del cliente, a quien se entregará, en su caso, al finalizar el servicio, así como a disposición de las autoridades policiales competentes para la inspección, en los términos previstos en el artículo 54.5.

4. Los informes de investigación deberán conservarse archivados, al menos, durante tres años, sin perjuicio de lo dispuesto en el artículo 16.3 de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Las imágenes y los sonidos grabados durante las investigaciones se destruirán tres años después de su finalización, salvo que estén relacionadas con un procedimiento judicial, una investigación policial o un procedimiento sancionador. En todo caso, el tratamiento de dichas imágenes y sonidos deberá observar lo establecido en la normativa sobre protección de datos de carácter personal, especialmente sobre el bloqueo de datos previsto en la misma.

5. Las investigaciones privadas tendrán carácter reservado y los datos obtenidos a través de las mismas solo se podrán poner a disposición del cliente o, en su caso, de los órganos judiciales y policiales, en este último supuesto únicamente para una investigación policial o para un procedimiento sancionador, conforme a lo dispuesto en el artículo 25.

Artículo 50. *Deber de reserva profesional.*

1. Los detectives privados están obligados a guardar reserva sobre las investigaciones que realicen, y no podrán facilitar datos o informaciones sobre éstas más que a las personas que se las encomendaron y a los órganos judiciales y policiales competentes para el ejercicio de sus funciones.

2. Sólo mediante requerimiento judicial o solicitud policial relacionada con el ejercicio de sus funciones en el curso de una investigación criminal o de un procedimiento sancionador se podrá acceder al contenido de las investigaciones realizadas por los detectives privados.

CAPÍTULO IV

Medidas de seguridad privada

Artículo 51. *Adopción de medidas.*

1. Las personas físicas o jurídicas, públicas o privadas, podrán dotarse de medidas de seguridad privada dirigidas a la protección de personas y bienes y al aseguramiento del normal desarrollo de sus actividades personales o empresariales.

2. Reglamentariamente, con la finalidad de prevenir la comisión de actos delictivos contra ellos o por generar riesgos directos para terceros o ser especialmente vulnerables, se determinarán los establecimientos e instalaciones industriales, comerciales y de servicios y los eventos que resulten obligados a adoptar medidas de seguridad, así como el tipo y características de las que deban implantar en cada caso.

3. El Ministerio del Interior o, en su caso, el órgano autonómico competente podrá ordenar que los titulares de establecimientos o instalaciones industriales, comerciales y de servicios y los organizadores de eventos adopten las medidas de seguridad que reglamentariamente se establezcan.

El órgano competente formulará la propuesta teniendo en cuenta, además de su finalidad preventiva de hechos delictivos y de evitación de riesgos, la naturaleza de la actividad, la localización de los establecimientos o instalaciones, la concentración de personas u otras circunstancias que la justifiquen y, previa audiencia del titular u organizador, resolverá motivadamente.

Cuando se considerase necesaria la implantación de dichas medidas en órganos u organismos públicos, el órgano competente formulará la correspondiente propuesta y, previo acuerdo con el órgano administrativo o entidad de los que dependan las instalaciones o locales necesitados de protección, dictará la resolución procedente.

4. Las sedes y delegaciones de las empresas de seguridad privada vinculadas a la operativa de seguridad y los despachos de detectives privados y sus sucursales estarán obligados a adoptar las medidas de seguridad que se establezcan reglamentariamente.

5. La celebración de eventos y la apertura o funcionamiento de establecimientos e instalaciones y de empresas de seguridad y sus delegaciones y despachos de detectives y sus sucursales, mencionados en los apartados 2 y 3, estará condicionada a la efectiva implantación de las medidas de seguridad que resulten obligatorias en cada caso.

6. Los órganos competentes podrán eximir de la implantación de medidas de seguridad obligatorias cuando las circunstancias que concurran en el caso concreto las hicieren innecesarias o improcedentes.

7. Los titulares de los establecimientos, instalaciones y empresas de seguridad privada y sus delegaciones, así como de los despachos de detectives privados y sus sucursales y los organizadores de eventos, serán responsables de la adopción de las medidas de seguridad que resulten obligatorias en cada caso.

Las empresas de seguridad encargadas de la prestación de las medidas de seguridad que les sean contratadas, serán responsables de su correcta instalación, mantenimiento y funcionamiento, sin perjuicio de la responsabilidad en que puedan incurrir sus empleados o los titulares de los establecimientos, instalaciones u organizadores obligados, si cualquier anomalía en su funcionamiento les fuera imputable.

8. Quedarán sometidos a lo establecido en esta ley y en sus disposiciones de desarrollo los usuarios que, sin estar obligados, adopten medidas de seguridad, así como quienes adopten medidas de seguridad adicionales a las obligatorias, respecto de éstas.

Artículo 52. *Tipos de medidas.*

1. A los exclusivos efectos de esta ley, se podrán adoptar los siguientes tipos de medidas de seguridad, destinadas a la protección de personas y bienes:

a) De seguridad física, cuya funcionalidad consiste en impedir o dificultar el acceso a determinados lugares o bienes mediante la interposición de cualquier tipo de barreras físicas.

b) De seguridad electrónica, orientadas a detectar o advertir cualquier tipo de amenaza, peligro, presencia o intento de asalto o intrusión que pudiera producirse, mediante la activación de cualquier tipo de dispositivos electrónicos.

c) De seguridad informática, cuyo objeto es la protección y salvaguarda de la integridad, confidencialidad y disponibilidad de los sistemas de información y comunicación, y de la información en ellos contenida.

d) De seguridad organizativa, dirigidas a evitar o poner término a cualquier tipo de amenaza, peligro o ataque deliberado, mediante la disposición, programación o planificación de cometidos, funciones o tareas formalizadas o ejecutadas por personas; tales como la

creación, existencia y funcionamiento de departamentos de seguridad o la elaboración y aplicación de todo tipo de planes de seguridad, así como cualesquiera otras de similar naturaleza que puedan adoptarse.

e) De seguridad personal, para la prestación de servicios de seguridad regulados en esta ley, distintos de los que constituyen el objeto específico de las anteriores.

2. Las características, elementos y finalidades de las medidas de seguridad de cualquier tipo, quien quiera que los utilice, se regularán reglamentariamente de acuerdo con lo previsto, en cuanto a sus grados y características, en las normas que contienen especificaciones técnicas para una actividad o producto. Asimismo dichas medidas de seguridad, medios materiales y sistemas de alarma deberán contar con la evaluación de los organismos de certificación acreditados en el momento de su instalación y tendrán vigencia indefinida, salvo deterioro o instalación de un nuevo sistema, que deberá ser conforme a la homologación que le resulte aplicable.

TÍTULO V

Control administrativo

Artículo 53. *Actuaciones de control.*

1. Corresponde a las Fuerzas y Cuerpos de Seguridad competentes en el ejercicio de las funciones de control de las empresas, despachos de detectives, de sus servicios o actuaciones y de su personal y medios en materia de seguridad privada, el cumplimiento de las órdenes e instrucciones que se impartan por los órganos a los que se refieren los artículos 12 y 13.

2. En el ejercicio de estas funciones, los miembros de las Fuerzas y Cuerpos de Seguridad competentes podrán requerir la información pertinente y adoptar las medidas provisionales que resulten necesarias, en los términos del artículo 55.

3. Cuando en el ejercicio de las actuaciones de control se detectase la posible comisión de una infracción administrativa, se instará a la autoridad competente para la incoación del correspondiente procedimiento sancionador. Si se tratara de la posible comisión de un hecho delictivo, se pondrá inmediatamente en conocimiento de la autoridad judicial.

4. Toda persona que tuviera conocimiento de irregularidades cometidas en el ámbito de la seguridad privada podrá denunciarlas ante las autoridades o funcionarios competentes, a efectos del posible ejercicio de las actuaciones de control y sanción correspondientes.

5. El acceso por los órganos que tengan atribuida la competencia de control se limitará a los datos necesarios para la realización de la misma.

Artículo 54. *Actuaciones de inspección.*

1. Las Fuerzas y Cuerpos de Seguridad competentes establecerán planes anuales de inspección ordinaria sobre las empresas, los despachos de detectives privados, el personal, los servicios, los establecimientos, los centros de formación, las medidas de seguridad y cualesquiera otras actividades o servicios regulados en esta ley.

2. Al margen de los citados planes de inspección, cuando recibieren denuncias sobre irregularidades cometidas en el ámbito de la seguridad privada procederán a la comprobación de los hechos denunciados y, en su caso, a instar la incoación del correspondiente procedimiento sancionador.

3. A los efectos anteriormente indicados, las empresas de seguridad, los despachos de detectives y el personal de seguridad privada, así como los establecimientos obligados a contratar servicios de seguridad privada, los centros de formación, las centrales de alarma de uso propio y los usuarios que contraten dichos servicios, habrán de facilitar a las Fuerzas y Cuerpos de Seguridad competentes el acceso a sus instalaciones y medios a efectos de inspección, así como a la información contenida en los contratos de seguridad, en los informes de investigación y en los libros-registro, en los supuestos y en la forma que reglamentariamente se determine.

4. Las actuaciones de inspección se atendrán a los principios de injerencia mínima y proporcionalidad, y tendrán por finalidad la comprobación del cumplimiento de la legislación aplicable.

5. Cuando las actuaciones de inspección recaigan sobre los servicios de investigación privada se tendrá especial cuidado en su ejecución, extremándose las cautelas en relación con las imágenes, sonidos o datos personales obtenidos que obren en el expediente de investigación. Las actuaciones se limitarán a la comprobación de su existencia, sin entrar en su contenido, salvo que se encuentre relacionado con una investigación judicial o policial o con un expediente sancionador.

6. Las inspecciones a las que se refieren los apartados anteriores se realizarán por el Cuerpo Nacional de Policía; por la Guardia Civil, en el caso de los guardas rurales y sus especialidades y centros y cursos de formación relativos a este personal; o, por el cuerpo de policía autonómica competente.

7. Siempre que el personal indicado en el apartado anterior realice una inspección, extenderá el acta correspondiente y, en el caso de existencia de infracción, se dará cuenta a la autoridad competente.

8. El acceso por los órganos que tengan atribuida la competencia de inspección se limitará a los datos necesarios para la realización de la misma.

Artículo 55. *Medidas provisionales anteriores al procedimiento.*

1. Los miembros de las Fuerzas y Cuerpos de Seguridad competentes podrán acordar excepcionalmente las siguientes medidas provisionales anteriores a la eventual incoación de un procedimiento sancionador, dando cuenta de ello inmediatamente a la autoridad competente:

a) La ocupación o precinto de vehículos, armas, material o equipos prohibidos, no homologados o que resulten peligrosos o perjudiciales, así como de los instrumentos y efectos de la infracción, en supuestos de grave riesgo o peligro inminente para las personas o bienes.

b) La suspensión, junto con la intervención u ocupación de los medios o instrumentos que se estuvieren empleando, de aquellos servicios de seguridad que se estuvieren prestando sin las preceptivas garantías y formalidades legales o sin contar con la necesaria autorización o declaración responsable, o cuando puedan causar daños o perjuicios a terceros o poner en peligro la seguridad ciudadana.

c) El cese de los servicios de seguridad cuando se constate que están siendo prestados por empresas, centrales de alarma de uso propio o despachos de detectives, no autorizados o que no hubieran presentado la declaración responsable, o por personal no habilitado o acreditado para el ejercicio legal de los mismos.

d) El cese de la actividad docente en materia de seguridad privada, cuando se constate que los centros que la imparten, no hayan presentado la declaración responsable o el profesorado no tuviera la acreditación correspondiente.

e) La desconexión de los sistemas de alarma cuyo mal funcionamiento causare perjuicios a la seguridad pública o molestias a terceros. Cuando se trate de establecimientos obligados a contar con esta medida de seguridad, la desconexión se suplirá mediante el establecimiento de un servicio permanente de vigilancia y protección privada.

f) La retirada de la tarjeta de identificación profesional al personal de seguridad o de la acreditación al personal acreditado, cuando resulten detenidos por su implicación en la comisión de hechos delictivos.

g) La suspensión, parcial o total, de las actividades de los establecimientos que sean notoriamente vulnerables y no tengan en funcionamiento las medidas de seguridad obligatorias.

2. Estas medidas habrán de ser ratificadas, modificadas o revocadas en el plazo máximo de quince días. En todo caso quedarán sin efecto si, transcurrido dicho plazo, no se incoa el procedimiento sancionador o el acuerdo de incoación no contiene un pronunciamiento expreso acerca de las mismas. El órgano competente para ratificar, revocar o modificar las medidas provisionales será el competente para incoar el procedimiento sancionador.

3. La duración de las medidas contempladas en el apartado 1, que deberá ser notificada a los interesados, no podrá exceder de seis meses.

4. Asimismo, con independencia de las responsabilidades penales o administrativas a que hubiere lugar, los miembros de las Fuerzas y Cuerpos de Seguridad competentes se harán cargo de las armas que se porten o utilicen ilegalmente, siguiendo lo dispuesto al respecto en la normativa de armas.

TÍTULO VI

Régimen sancionador

CAPÍTULO I

Infracciones

Artículo 56. *Clasificación y prescripción.*

1. Las infracciones de las normas contenidas en esta ley podrán ser leves, graves y muy graves.

2. Las infracciones leves prescribirán a los seis meses, las graves al año y las muy graves a los dos años.

3. El plazo de prescripción se contará desde la fecha en que la infracción hubiera sido cometida. En las infracciones derivadas de una actividad continuada, la fecha inicial del cómputo será la de la finalización de la actividad o la del último acto en que la infracción se consume.

4. La prescripción se interrumpirá por la iniciación, con conocimiento del interesado, del procedimiento sancionador, volviendo a correr el plazo si el expediente permaneciera paralizado durante seis meses por causa no imputable a aquellos contra quienes se dirija.

Artículo 57. *Infracciones de las empresas que desarrollen actividades de seguridad privada, de sus representantes legales, de los despachos de detectives privados y de las centrales de alarma de uso propio.*

Las empresas que desarrollen actividades de seguridad privada, sus representantes legales, los despachos de detectives privados y las centrales de alarma de uso propio, podrán incurrir en las siguientes infracciones:

1. Infracciones muy graves:

a) La prestación de servicios de seguridad privada a terceros careciendo de autorización o, en su caso, sin haber presentado la declaración responsable prevista en el artículo 18.1 y 2 para la prestación de los servicios de que se trate.

b) La contratación o utilización, en servicios de seguridad privada, de personas que carezcan de la habilitación o acreditación correspondiente.

c) La realización de actividades prohibidas en el artículo 8.4, sobre reuniones o manifestaciones, conflictos políticos o laborales, control de opiniones o su expresión, o la información a terceras personas sobre bienes de cuya seguridad o investigación hubieran sido encargados, o cualquier otra forma de quebrantamiento del deber de reserva, cuando no sean constitutivas de delito y salvo que sean constitutivas de infracción a la normativa sobre protección de datos de carácter personal.

d) La instalación o utilización de medios materiales o técnicos no homologados cuando la homologación sea preceptiva y sean susceptibles de causar grave daño a las personas o a los intereses generales.

e) La negativa a facilitar, cuando proceda, la información contenida en los contratos de seguridad privada, en los libros-registro o el acceso a los informes de investigación privada.

f) El incumplimiento de las previsiones normativas sobre adquisición y uso de armas, así como sobre disponibilidad de armeros y custodia de aquéllas, particularmente la tenencia de armas por el personal a su servicio fuera de los casos permitidos por esta ley, o la contratación de instructores de tiro que carezcan de la oportuna habilitación.

g) La prestación de servicios de seguridad privada con armas de fuego fuera de lo dispuesto en esta ley.

h) La negativa a prestar auxilio o colaboración a las Fuerzas y Cuerpos de Seguridad en la investigación y persecución de actos delictivos; en el descubrimiento y detención de los delincuentes; o en la realización de las funciones inspectoras o de control que les correspondan.

i) El incumplimiento de la obligación que impone a los representantes legales el artículo 22.3.

j) La ausencia de las medidas de seguridad obligatorias, por parte de las empresas de seguridad privada y los despachos de detectives, en sus sedes, delegaciones y sucursales.

k) El incumplimiento de las condiciones de prestación de servicios establecidos por la autoridad competente en relación con el ejercicio del derecho de huelga en servicios esenciales, o en los que el servicio de seguridad se haya impuesto obligatoriamente, en los supuestos a que se refiere el artículo 8.6.

l) El incumplimiento de los requisitos que impone a las empresas de seguridad el artículo 19. 1, 2 y 3, y el artículo 35.2.

m) El incumplimiento de los requisitos que impone a los despachos de detectives el artículo 24. 1 y 2.

n) La falta de transmisión a las Fuerzas y Cuerpos de Seguridad competentes de las alarmas reales que se registren en las centrales receptoras de alarmas privadas, incluidas las de uso propio, así como el retraso en la transmisión de las mismas, cuando estas conductas no estén justificadas.

ñ) La prestación de servicios compatibles contemplados en el artículo 6.2, empleando personal no habilitado que utilice armas o medios de defensa reservados al personal de seguridad privada.

o) La realización de investigaciones privadas a favor de solicitantes en los que no concurra un interés legítimo en el asunto.

p) La prestación de servicios de seguridad privada sin formalizar los correspondientes contratos.

q) El empleo o utilización, en servicios de seguridad privada, de medidas o de medios personales, materiales o técnicos de forma que se atente contra el derecho al honor, a la intimidad personal o familiar o a la propia imagen o al secreto de las comunicaciones, siempre que no constituyan delito.

r) La falta de comunicación por parte de empresas de seguridad informática de las incidencias relativas al sistema de cuya protección sean responsables cuando sea preceptivo.

s) La comisión de una tercera infracción grave o de una grave y otra muy grave en el período de dos años, habiendo sido sancionado por las anteriores.

t) La prestación de actividades ajenas a las de seguridad privada, excepto las compatibles previstas en el artículo 6 de la presente ley.

2. Infracciones graves:

a) La instalación o utilización de medios materiales o técnicos no homologados, cuando la homologación sea preceptiva.

b) La prestación de servicios de seguridad privada con vehículos, uniformes, distintivos, armas o medios de defensa que no reúnan las características reglamentarias.

c) La prestación de servicios de seguridad privada careciendo de los requisitos específicos de autorización o presentación de declaración responsable para la realización de dicho tipo de servicios. Esta infracción también será aplicable cuando tales servicios se lleven a cabo fuera del lugar o del ámbito territorial para el que estén autorizados o se haya presentado la declaración responsable, o careciendo de la autorización previa o de dicha declaración cuando éstas sean preceptivas, o cuando se realicen en condiciones distintas a las expresamente previstas en la autorización del servicio.

d) La retención de la documentación profesional del personal de seguridad privada, o de la acreditación del personal acreditado.

e) La prestación de servicios de seguridad privada sin comunicar correctamente los correspondientes contratos al Ministerio del Interior o al órgano autonómico competente, o

en los casos en que la comunicación se haya producido con posterioridad al inicio del servicio.

f) La prestación de servicios de seguridad privada sin cumplir lo estipulado en el correspondiente contrato.

g) La falta de sustitución ante el abandono o la omisión injustificados del servicio por parte del personal de seguridad privada, dentro de la jornada laboral establecida.

h) La utilización, en el desempeño de funciones de seguridad privada, de personal de seguridad privada, con una antigüedad mínima de un año en la empresa, que no haya realizado los correspondientes cursos de actualización o especialización, no los haya superado, o no los haya realizado con la periodicidad que reglamentariamente se determine.

i) La falta de presentación al Ministerio del Interior o al órgano autonómico competente del certificado acreditativo de la vigencia del contrato de seguro, aval o seguro de caución en los términos establecidos en el artículo 19.1.e) y f) y 24.2.e) y f), así como la no presentación del informe de actividades y el resumen de la cuenta anual a los que se refiere el artículo 21.1.e), o la no presentación de la memoria a la que se refiere el artículo 25.1.i)

j) La comunicación de una o más falsas alarmas por negligencia, deficiente funcionamiento o falta de verificación previa.

k) La apertura de delegaciones o sucursales sin obtener la autorización necesaria o sin haber presentado la declaración responsable ante el órgano competente, cuando sea preceptivo.

l) La falta de comunicación al Ministerio del Interior o, en su caso, al órgano autonómico competente, de las altas y bajas del personal de seguridad privada, así como de los cambios que se produzcan en sus representantes legales y toda variación en la composición personal de los órganos de administración, gestión, representación y dirección.

m) La prestación de servicio por parte del personal de seguridad privada sin la debida uniformidad o sin los medios que reglamentariamente sean exigibles.

n) La no realización de las revisiones anuales obligatorias de los sistemas o medidas de seguridad cuyo mantenimiento tuvieren contratado.

ñ) La carencia o falta de cumplimentación de cualquiera de los libros-registro obligatorios.

o) La falta de comunicación al Ministerio del Interior o, en su caso, al órgano autonómico competente de todo cambio relativo a su personalidad o forma jurídica, denominación, número de identificación fiscal o domicilio.

p) La falta de mantenimiento, en todo momento, de los requisitos establecidos para los representantes legales en el artículo 22.2.

q) El deficiente funcionamiento, por parte de las empresas de seguridad privada y despachos de detectives, en sus sedes, delegaciones o sucursales, de las medidas de seguridad obligatorias, así como el incumplimiento de las revisiones obligatorias de las mismas.

r) La prestación de servicios compatibles contemplados en el artículo 6.2 empleando personal no habilitado que utilice distintivos, uniformes o medios que puedan confundirse con los del personal de seguridad privada.

s) El incumplimiento de los requisitos impuestos a las empresas de seguridad informática.

t) La prestación de servicios incumpliendo lo dispuesto en el artículo 19.4.

u) La actuación de vigilantes de seguridad en el exterior de las instalaciones, inmuebles o propiedades de cuya vigilancia o protección estuvieran encargadas las empresas de seguridad privada con motivo de la prestación de servicios de tal naturaleza, fuera de los supuestos legalmente previstos.

v) No depositar la documentación profesional sobre contratos, informes de investigación y libros-registros en las dependencias del Cuerpo Nacional de Policía o, en su caso, del cuerpo de policía autonómico competente, en caso de cierre del despacho de detectives privados.

w) La comisión de una tercera infracción leve o de una grave y otra leve, en el período de dos años, habiendo recaído sanción por las anteriores.

x) La publicidad de servicios de seguridad privada por parte de personas, físicas o jurídicas, carentes de la correspondiente autorización o sin haber presentado declaración responsable.

y) La prestación de servicios de seguridad privada en condiciones distintas a las previstas en las comunicaciones de los correspondientes contratos.

3. Infracciones leves:

a) El incumplimiento de la periodicidad de las revisiones obligatorias de los sistemas o medidas de seguridad cuyo mantenimiento tuvieren contratado.

b) La utilización en los servicios de seguridad privada de vehículos, uniformes o distintivos con apariencia o semejanza a los de las Fuerzas y Cuerpos de Seguridad o de las Fuerzas Armadas.

c) La falta de diligencia en la cumplimentación de los libros-registro obligatorios.

d) En general, el incumplimiento de los trámites, condiciones o formalidades establecidos por esta ley, siempre que no constituya infracción grave o muy grave.

Artículo 58. *Infracciones del personal que desempeñe funciones de seguridad privada.*

El personal que desempeñe funciones de seguridad privada, así como los ingenieros, técnicos, operadores de seguridad y profesores acreditados, podrán incurrir en las siguientes infracciones:

1. Infracciones muy graves:

a) El ejercicio de funciones de seguridad privada para terceros careciendo de la habilitación o acreditación necesaria.

b) El incumplimiento de las previsiones contenidas en esta ley sobre tenencia de armas de fuego fuera del servicio y sobre su utilización.

c) La falta de reserva debida sobre los hechos que conozcan en el ejercicio de sus funciones o la utilización de medios materiales o técnicos de tal forma que atenten contra el derecho al honor, a la intimidad personal o familiar, a la propia imagen o al secreto de las comunicaciones cuando no constituyan delito.

d) La negativa a prestar auxilio o colaboración a las Fuerzas y Cuerpos de Seguridad, cuando sea procedente, en la investigación y persecución de actos delictivos; en el descubrimiento y detención de los delincuentes; o en la realización de las funciones inspectoras o de control que les correspondan.

e) La negativa a identificarse profesionalmente, en el ejercicio de sus respectivas funciones, ante la Autoridad o sus agentes, cuando fueren requeridos para ello.

f) La realización de investigaciones sobre delitos perseguibles de oficio o la falta de denuncia a la autoridad competente de los delitos que conozcan los detectives privados en el ejercicio de sus funciones.

g) La realización de actividades prohibidas en el artículo 8.4 sobre reuniones o manifestaciones, conflictos políticos y laborales, control de opiniones o su expresión, o la información a terceras personas sobre bienes de cuya seguridad estén encargados, en el caso de que no sean constitutivas de delito; salvo que sean constitutivas infracción a la normativa sobre protección de datos de carácter personal.

h) El ejercicio abusivo de sus funciones en relación con los ciudadanos.

i) La realización, orden o tolerancia, en el ejercicio de su actuación profesional, de prácticas abusivas, arbitrarias o discriminatorias, incluido el acoso, que entrañen violencia física o moral, cuando no constituyan delito.

j) El abandono o la omisión injustificados del servicio por parte del personal de seguridad privada, dentro de la jornada laboral establecida.

k) La elaboración de proyectos o ejecución de instalaciones o mantenimientos de sistemas de seguridad conectados a centrales receptoras de alarmas, centros de control o de videovigilancia, sin disponer de la acreditación correspondiente expedida por el Ministerio del Interior.

l) La no realización del informe de investigación que preceptivamente deben elaborar los detectives privados o su no entrega al contratante del servicio, o la elaboración de informes paralelos.

m) El ejercicio de funciones de seguridad privada por parte del personal a que se refiere el artículo 28.3 y 4.

n) La comisión de una tercera infracción grave o de una grave y otra muy grave en el período de dos años, habiendo sido sancionado por las anteriores.

2. Infracciones graves:

a) La realización de funciones de seguridad privada que excedan de la habilitación obtenida.

b) El ejercicio de funciones de seguridad privada por personal habilitado, no integrado en empresas de seguridad privada, o en la plantilla de la empresa, cuando resulte preceptivo conforme a lo dispuesto en el artículo 38.5, o al margen de los despachos de detectives.

c) La falta de respeto al honor o a la dignidad de las personas.

d) El ejercicio del derecho a la huelga al margen de lo dispuesto al respecto para los servicios que resulten o se declaren esenciales por la autoridad pública competente, o en los que el servicio de seguridad se haya impuesto obligatoriamente, en los supuestos a que se refiere el artículo 8.6.

e) La no identificación profesional, en el ejercicio de sus respectivas funciones, cuando fueren requeridos para ello por los ciudadanos.

f) La retención de la documentación personal en contra de lo previsto en el artículo 32.1.b).

g) La falta de diligencia en el cumplimiento de las respectivas funciones por parte del personal habilitado o acreditado.

h) La identificación profesional haciendo uso de documentos o distintivos diferentes a los dispuestos legalmente para ello o acompañando éstos con emblemas o distintivos de apariencia semejante a los de las Fuerzas y Cuerpos de Seguridad o de las Fuerzas Armadas.

i) La negativa a realizar los cursos de formación permanente a los que vienen obligados.

j) La elaboración de proyectos o ejecución de instalaciones o mantenimientos de sistemas de seguridad conectados a centrales receptoras de alarmas, centros de control o de videovigilancia, no ajustados a las normas técnicas reglamentariamente establecidas.

k) La omisión, total o parcial, de los datos que obligatoriamente debe contener el informe de investigación que deben elaborar los detectives privados.

l) El ejercicio de funciones de seguridad privada incompatibles entre sí, por parte de personal habilitado para ellas.

m) La comisión de una tercera infracción leve o de una grave y otra leve, en el período de dos años, habiendo recaído sanción por las anteriores.

n) La validación provisional de sistemas o medidas de seguridad que no se adecuen a la normativa de seguridad privada.

3. Infracciones leves:

a) La actuación sin la debida uniformidad o medios, que reglamentariamente sean exigibles, o sin portar los distintivos o la documentación profesional, así como la correspondiente al arma de fuego utilizada en la prestación del servicio encomendado.

b) El trato incorrecto o desconsiderado con los ciudadanos.

c) La no cumplimentación, total o parcial, por parte de los técnicos acreditados, del documento justificativo de las revisiones obligatorias de los sistemas de seguridad conectados a centrales receptoras de alarmas, centros de control o de videovigilancia.

d) En general, el incumplimiento de los trámites, condiciones o formalidades establecidos por esta ley, siempre que no constituya infracción grave o muy grave.

Artículo 59. *Infracciones de los usuarios y centros de formación.*

Los usuarios de servicios de seguridad privada y los centros de formación de personal de seguridad privada podrán incurrir en las siguientes infracciones:

1. Muy graves:

a) La contratación o utilización a sabiendas de los servicios de empresas de seguridad o despachos de detectives carentes de la autorización específica o declaración responsable necesaria para el desarrollo de los servicios de seguridad privada.

b) La utilización de aparatos de alarmas u otros dispositivos de seguridad no homologados cuando fueran susceptibles de causar grave daño a las personas o a los intereses generales.

c) El incumplimiento, por parte de los centros de formación, de los requisitos y condiciones exigidos en la declaración responsable, o impartir cursos sin haberla presentado.

d) La negativa a prestar auxilio o colaboración a las Fuerzas y Cuerpos de Seguridad competentes en la realización de las funciones inspectoras de las medidas de seguridad, de los centros de formación y de los establecimientos obligados.

e) La no adecuación de los cursos que se impartan en los centros de formación a lo previsto reglamentariamente en cuanto a su duración, modalidades y contenido.

f) La falta de adopción o instalación de las medidas de seguridad que resulten obligatorias.

g) La falta de comunicación de las incidencias detectadas y confirmadas en su centro de control de la seguridad de la información y las comunicaciones, cuando sea preceptivo.

h) La contratación o utilización a sabiendas de personas carentes de la habilitación o acreditación necesarias para la prestación de servicios de seguridad o la utilización de personal docente no acreditado en actividades de formación.

i) La comisión de una tercera infracción grave o de una grave y otra muy grave en el período de dos años, habiendo sido sancionado por las anteriores.

j) La entrada en funcionamiento, sin previa autorización, de centrales receptoras de alarmas de uso propio por parte de entidades públicas o privadas.

k) Obligar a personal habilitado contratado a realizar otras funciones distintas a aquellas para las que fue contratado.

2. Graves:

a) El incumplimiento de las revisiones preceptivas de los sistemas o medidas de seguridad obligatorias que tengan instalados.

b) La utilización de aparatos de alarma u otros dispositivos de seguridad no homologados.

c) La no comunicación al órgano competente de las modificaciones que afecten a cualquiera de los requisitos que dieron lugar a la autorización de los centros de formación.

d) La impartición de los cursos de formación fuera de las instalaciones autorizadas de los centros de formación.

e) El anormal funcionamiento de las medidas de seguridad obligatorias adoptadas o instaladas cuando ocasionen perjuicios a la seguridad pública o a terceros.

f) La utilización de personal docente no acreditado en actividades de formación.

g) La comisión de una tercera infracción leve o de una grave y otra leve, en el período de dos años, habiendo recaído sanción por las anteriores.

h) El incumplimiento, por parte de los usuarios de seguridad privada, de la obligación de situar al frente de la seguridad integral de la entidad, empresa o grupo empresarial a un director de seguridad, en contra de lo previsto en el artículo 36.2.

3. Leves:

a) La utilización de aparatos o dispositivos de seguridad sin ajustarse a las normas que los regulen, o cuando su funcionamiento cause daños o molestias desproporcionados a terceros.

b) El anormal funcionamiento de las medidas o sistemas de seguridad que se tengan instalados.

c) Las irregularidades en la cumplimentación de los registros prevenidos.

d) En general, el incumplimiento de las obligaciones contenidas en esta ley que no constituya infracción grave o muy grave.

Artículo 60. *Colaboración reglamentaria.*

Las disposiciones reglamentarias de desarrollo podrán introducir especificaciones o graduaciones en el cuadro de las infracciones y sanciones establecidas en esta ley que, sin constituir nuevas infracciones o sanciones, ni alterar la naturaleza o límites de las que en ella se contemplan, contribuyan a la más correcta identificación de las conductas o a la más precisa determinación de las sanciones correspondientes.

CAPÍTULO II

Sanciones

Artículo 61. *Sanciones a las empresas que desarrollen actividades de seguridad privada, sus representantes legales, los despachos de detectives privados y las centrales de alarma de uso propio.*

Las autoridades competentes podrán imponer, por la comisión de las infracciones tipificadas en el artículo 57, las siguientes sanciones:

1. Por la comisión de infracciones muy graves:

a) Multa de 30.001 a 600.000 euros.
b) Extinción de la autorización, o cierre de la empresa o despacho en los casos de declaración responsable, que comportará la prohibición de volver a obtenerla o presentarla, respectivamente, por un plazo de entre uno y dos años, y cancelación de la inscripción en el registro correspondiente.
c) Prohibición para ocupar cargos de representación legal en empresas de seguridad privada por un plazo de entre uno y dos años.

2. Por la comisión de infracciones graves:

a) Multa de 3.001 a 30.000 euros.
b) Suspensión temporal de la autorización o de la declaración responsable por un plazo de entre seis meses y un año.
c) Prohibición para ocupar cargos de representación legal en empresas de seguridad privada por un plazo de entre seis meses y un año.

3. Por la comisión de infracciones leves:

a) Apercibimiento.
b) Multa de 300 a 3.000 euros.

Artículo 62. *Sanciones al personal.*

Las autoridades competentes podrán imponer, por la comisión de las infracciones tipificadas en el artículo 58, las siguientes sanciones:

1. Por la comisión de infracciones muy graves:

a) Multa de 6.001 a 30.000 euros.
b) Extinción de la habilitación, que comportará la prohibición de volver a obtenerla por un plazo de entre uno y dos años, y cancelación de la inscripción en el Registro Nacional.

2. Por la comisión de infracciones graves:

a) Multa de 1.001 a 6.000 euros.
b) Suspensión temporal de la habilitación por un plazo de entre seis meses y un año.

3. Por la comisión de infracciones leves:

a) Apercibimiento.
b) Multa de 300 a 1.000 euros.

Artículo 63. *Sanciones a usuarios y centros de formación.*

Las autoridades competentes podrán imponer, por la comisión de las infracciones tipificadas en el artículo 59, las siguientes sanciones:

1. Por la comisión de infracciones muy graves:

a) Multa de 20.001 a 100.000 euros.
b) Cierre del centro de formación, que comportará la prohibición de volver a presentar la declaración responsable para su apertura por un plazo de entre uno y dos años, y cancelación de la inscripción en el registro correspondiente.
c) La clausura, desde seis meses y un día a dos años, de los establecimientos que no tengan en funcionamiento las medidas de seguridad obligatorias.

2. Por la comisión de infracciones graves:

a) Multa de 3.001 a 20.000 euros.
b) Suspensión temporal de la declaración responsable del centro de formación por un plazo de entre seis meses y un año.

3. Por la comisión de infracciones leves:

a) Apercibimiento.
b) Multa de 300 a 3.000 euros.

Artículo 64. *Graduación de las sanciones.*

Para la graduación de las sanciones, los órganos competentes tendrán en cuenta la gravedad y trascendencia del hecho, el posible perjuicio para el interés público, la situación de riesgo creada o mantenida para personas o bienes, la reincidencia, la intencionalidad, el volumen de actividad de la empresa de seguridad, despacho de detectives, centro de formación o establecimiento contra el que se dicte la resolución sancionadora, y la capacidad económica del infractor.

Artículo 65. *Aplicación de las sanciones.*

1. Las sanciones previstas en esta ley podrán aplicarse de forma alternativa o acumulativa.
2. La aplicación de sanciones pecuniarias tenderá a evitar que la comisión de las infracciones tipificadas no resulte más beneficiosa para el infractor que el cumplimiento de las normas infringidas.

Artículo 66. *Competencia sancionadora.*

1. En el ámbito de la Administración General del Estado, la potestad sancionadora corresponderá:

a) Al Ministro del Interior, para imponer las sanciones de extinción de las autorizaciones, habilitaciones y declaraciones responsables.
b) Al Secretario de Estado de Seguridad, para imponer las restantes sanciones por infracciones muy graves.
c) Al Director General de la Policía, para imponer las sanciones por infracciones graves.
Cuando, en el curso de las inspecciones por parte de la Guardia Civil de los cursos para guardas rurales, impartidos por centros de formación no exclusivos de éstos, se detecten posibles infracciones, la sanción corresponderá al Director General de la Policía.
d) Al Director General de la Guardia Civil, para imponer las sanciones por infracciones graves en relación con los guardas rurales y centros y cursos de formación exclusivos para este personal.
e) A los Delegados y a los Subdelegados del Gobierno, para imponer las sanciones por infracciones leves.

2. En el ámbito de las comunidades autónomas con competencia en materia de seguridad privada, la potestad sancionadora corresponderá a los titulares de los órganos que se determinen en cada caso.

3. Contra las resoluciones sancionadoras se podrán interponer los recursos previstos en la legislación de procedimiento administrativo y en la de la jurisdicción contencioso-administrativa.

Artículo 67. *Decomiso del material.*

El material prohibido, no homologado o indebidamente utilizado en servicios de seguridad privada, será decomisado y se procederá a su destrucción si no fuera de lícito comercio, o a su enajenación en otro caso, quedando en depósito la cantidad que se obtuviera para hacer frente a las responsabilidades administrativas o de otro orden en que se haya podido incurrir.

Artículo 68. *Prescripción de las sanciones.*

1. Las sanciones impuestas por infracciones leves, graves o muy graves prescribirán, respectivamente, al año, a los dos años y a los cuatro años.
2. El plazo de prescripción comenzará a contarse desde el día siguiente a aquel en que sea firme la resolución por la que se impone la sanción, si ésta no se hubiese comenzado a ejecutar, o desde que se quebrantase el cumplimiento de la misma, si hubiese comenzado, y se interrumpirá desde que se comience o se reanude la ejecución o cumplimiento.

CAPÍTULO III

Procedimiento

Artículo 69. *Régimen Jurídico.*

1. El ejercicio de la potestad sancionadora en materia de seguridad privada se regirá por lo dispuesto en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y sus disposiciones de desarrollo, sin perjuicio de las especialidades que se regulan en este título.
2. El procedimiento caducará transcurridos seis meses desde su incoación sin que se haya notificado la resolución, debiendo, no obstante, tenerse en cuenta en el cómputo las posibles paralizaciones por causas imputables al interesado o la suspensión que debiera acordarse por la existencia de un procedimiento judicial penal, cuando concurra identidad de sujeto, hecho y fundamento, hasta la finalización de éste.
3. Iniciado el procedimiento sancionador, el órgano que haya ordenado su incoación podrá adoptar las medidas cautelares necesarias para garantizar su adecuada instrucción, así como para evitar la continuación de la infracción o asegurar el pago de la sanción, en el caso de que ésta fuese pecuniaria, y el cumplimiento de la misma en los demás supuestos.
4. Dichas medidas, que deberán ser congruentes con la naturaleza de la presunta infracción y proporcionadas a la gravedad de la misma, podrán consistir en:

a) La ocupación o precinto de vehículos, armas, material o equipo prohibido, no homologado o que resulte peligroso o perjudicial, así como de los instrumentos y efectos de la infracción.
b) La retirada preventiva de las autorizaciones, habilitaciones, permisos o licencias, o la suspensión, en su caso, de la eficacia de las declaraciones responsables.
c) La suspensión de la habilitación del personal de seguridad privada y, en su caso, de la tramitación del procedimiento para el otorgamiento de aquélla, mientras dure la instrucción de expedientes por infracciones graves o muy graves en materia de seguridad privada.
También podrán ser suspendidas las indicadas habilitación y tramitación, hasta tanto finalice el proceso por delitos contra dicho personal.

5. Las medidas cautelares previstas en los párrafos b) y c) del apartado anterior no podrán tener una duración superior a un año.

Artículo 70. *Ejecutoriedad.*

1. Las sanciones impuestas serán inmediatamente ejecutivas desde que la resolución adquiera firmeza en vía administrativa.
2. Cuando la sanción sea de naturaleza pecuniaria y no se haya previsto plazo para satisfacerla, la autoridad que la impuso lo señalará, sin que pueda ser inferior a quince ni superior a treinta días hábiles, pudiendo acordarse el fraccionamiento del pago.
3. En los casos de suspensión temporal y extinción de la eficacia de autorizaciones, habilitaciones o declaraciones responsables y prohibición del ejercicio de la representación legal de las empresas, la autoridad sancionadora señalará un plazo de ejecución suficiente, que no podrá ser inferior a quince días hábiles ni superior a dos meses, oyendo al sancionado y a los terceros que pudieran resultar directamente afectados.

Artículo 71. *Publicidad de las sanciones.*

Las sanciones, así como los nombres, apellidos, denominación o razón social de las personas físicas o jurídicas responsables de la comisión de infracciones muy graves, cuando hayan adquirido firmeza en vía administrativa, podrán ser hechas públicas, en virtud de acuerdo de la autoridad competente para su imposición, siempre que concurra riesgo para la seguridad de los usuarios o ciudadanos, reincidencia en infracciones de naturaleza análoga o acreditada intencionalidad.

Artículo 72. *Multas coercitivas.*

1. Para lograr el cumplimiento de las resoluciones sancionadoras, las autoridades competentes relacionadas en el artículo 66 podrán imponer multas coercitivas, de acuerdo con lo establecido en la legislación de procedimiento administrativo.
2. La cuantía de estas multas no excederá de 6.000 euros, pero podrá aumentarse sucesivamente en el 50 por 100 de la cantidad anterior en casos de reiteración del incumplimiento.
3. Las multas coercitivas serán independientes de las sanciones pecuniarias que puedan imponerse y compatibles con ellas.

Disposición adicional primera. *Comercialización de productos.*

En la comercialización de productos provenientes de los Estados miembros de la Unión Europea, del Espacio Económico Europeo o de cualquier tercer país con el que la Unión Europea tenga un acuerdo de asociación y que estén sometidos a reglamentaciones nacionales de seguridad, equivalentes a la reglamentación española de seguridad privada, se atenderá a los estándares previstos por las entidades de certificación acreditadas que ofrezcan, a través de su administración pública competente, garantías técnicas profesionales y de independencia e imparcialidad equivalentes a las exigidas por la legislación española, y a que las disposiciones del Estado, con base en las que se evalúa la conformidad, comporten un nivel de seguridad equivalente al exigido por las disposiciones legales aplicables.

Disposición adicional segunda. *Contratación de servicios de seguridad privada por las administraciones públicas.*

1. En consideración a la relevancia para la seguridad pública de los servicios de seguridad privada, de conformidad con el artículo 118 del texto refundido de la Ley de Contratos del Sector Público, aprobado por el Real Decreto Legislativo 3/2011, de 14 de noviembre, los órganos de contratación de las administraciones públicas podrán establecer condiciones especiales de ejecución de los contratos de servicios de seguridad relacionadas con el cumplimiento de las obligaciones laborales por parte de las empresas de seguridad privada contratistas.
2. Los pliegos de cláusulas administrativas particulares o los contratos podrán establecer penalidades para el caso de incumplimiento de estas condiciones especiales de ejecución, o atribuirles el carácter de obligaciones contractuales esenciales a los efectos de la resolución de los contratos, de acuerdo con los artículos 212.1 y 223.f).

Disposición adicional tercera. *Cooperación administrativa.*

En consideración a la relevancia para la seguridad pública de los servicios de seguridad privada, los órganos competentes en materia policial, tributaria, laboral y de seguridad social establecerán mecanismos de información, control e inspección conjunta en relación con las empresas de seguridad privada para evitar el fraude y el intrusismo.

Disposición transitoria primera. *Habilitaciones profesionales anteriores a la entrada en vigor de esta ley.*

1. Las habilitaciones del personal de seguridad privada obtenidas antes de la entrada en vigor de esta ley mantendrán su validez sin necesidad de convalidación o canje alguno.
2. Las habilitaciones correspondientes a los guardas particulares del campo se entenderán hechas a la nueva categoría de guardas rurales.

Disposición transitoria segunda. *Personal de centrales receptoras de alarmas.*

Quienes a la entrada en vigor de esta ley estuvieran desempeñando su actividad en centrales receptoras de alarmas, podrán continuar desarrollando sus funciones sin necesidad de obtener ninguna acreditación específica.

Disposición transitoria tercera. *Ingenieros y técnicos de las empresas de seguridad.*

Los ingenieros y técnicos encuadrados, en el momento de entrada en vigor de esta ley, en empresas de seguridad autorizadas para la actividad de instalación y mantenimiento de sistemas de seguridad contemplada en el artículo 5.1.f) podrán continuar desarrollando sus funciones sin necesidad de obtener la acreditación específica a la que se refiere el artículo 19.1.c).

Disposición transitoria cuarta. *Plazos de adecuación.*

1. Las empresas de seguridad privada y sus delegaciones, los despachos de detectives privados y sus sucursales, las medidas de seguridad adoptadas y el material o equipo en uso a la entrada en vigor de esta ley de acuerdo con la normativa anterior, pero que no cumplan, total o parcialmente, los requisitos o exigencias establecidos en esta ley y en sus normas de desarrollo, deberán adaptarse a tales requisitos y exigencias, dentro de los siguientes plazos de adecuación, computados a partir de su entrada en vigor:

a) Dos años respecto a los requisitos nuevos de las empresas de seguridad privada y sus delegaciones y de los despachos de detectives privados y sus sucursales.
b) Diez años para las medidas de seguridad electrónicas de las empresas de seguridad, de los establecimientos obligados y de las instalaciones de los usuarios no obligados.
c) Un año para la obtención de la certificación prevista en el artículo 19.4.

2. Las medidas de seguridad física instaladas con anterioridad a la entrada en vigor de esta ley tendrán una validez indefinida, hasta el final de su vida útil; no obstante, deberán ser actualizadas en caso de resultar afectadas por reformas estructurales de los sistemas de seguridad de los que formen parte.
3. Los sistemas de seguridad y los elementos de seguridad física, electrónica e informática que se instalen a partir de la entrada en vigor de esta ley deberán cumplir todas las exigencias y requisitos establecidos en la misma y en su normativa de desarrollo.

Disposición transitoria quinta. *Actividad de planificación y asesoramiento.*

1. Las empresas de seguridad autorizadas e inscritas únicamente para la actividad de planificación y asesoramiento contemplada en el artículo 5.1.g) de la Ley 23/1992, de 30 de julio, de Seguridad Privada, dispondrán de un plazo de tres meses, desde la entrada en vigor de esta ley, para solicitar autorización para cualquiera de las actividades enumeradas en el artículo 5.1 de la misma, excepto la contemplada en el párrafo h).
2. Las empresas de seguridad referidas en el apartado anterior que, transcurrido dicho plazo, no hubieran solicitado la mencionada autorización, serán dadas de baja de oficio,

cancelándose su inscripción en el Registro Nacional de Seguridad Privada y, en su caso, en el registro autonómico correspondiente.

3. En el caso de las empresas de seguridad que, a la entrada en vigor de esta ley, estuvieran autorizadas e inscritas para la actividad de planificación y asesoramiento y, además, para cualquier otra contemplada en el artículo 5.1, se cancelará de oficio su inscripción y autorización en el Registro Nacional de Seguridad Privada y, en su caso, en el registro autonómico correspondiente únicamente respecto a dicha actividad de planificación y asesoramiento.

4. Las empresas de seguridad referidas en el apartado anterior dispondrán de un plazo de un año, desde la entrada en vigor de esta ley, para adecuar los respectivos importes del seguro de responsabilidad civil u otra garantía financiera, así como del aval o seguro de caución, en función de las actividades para las que continúen autorizadas e inscritas en los registros correspondientes.

5. Los procedimientos administrativos que, a la entrada en vigor de esta ley, se estuvieran tramitando en relación con la solicitud de autorización e inscripción para desarrollar únicamente la referida actividad de planificación y asesoramiento se darán por terminados, procediéndose al archivo de las actuaciones.

6. Los procedimientos administrativos que, a la entrada en vigor de esta ley, se estuvieran tramitando en relación con la solicitud de autorización para desarrollar actividades de seguridad privada entre las que se incluya la referida actividad de planificación y asesoramiento, continuarán su tramitación en relación exclusivamente con el resto de actividades solicitadas.

Disposición derogatoria única. *Derogación normativa.*

1. Queda derogada la Ley 23/1992, de 30 de julio, de Seguridad Privada, y cuantas normas de igual o inferior rango se opongan a lo dispuesto en esta ley.

2. El Reglamento de Seguridad Privada, aprobado por el Real Decreto 2364/1994, de 9 de diciembre, y el resto de la normativa de desarrollo de la Ley 23/1992, de 30 de julio, y del propio Reglamento mantendrán su vigencia en lo que no contravenga a esta ley.

Disposición final primera. *Título competencial.*

Esta ley se dicta al amparo de lo dispuesto en el artículo 149.1.29.ª de la Constitución, que atribuye al Estado la competencia exclusiva en materia de seguridad pública.

Disposición final segunda. *Procedimiento administrativo.*

En todo lo no regulado expresamente en esta ley se aplicará la legislación sobre procedimiento administrativo.

Disposición final tercera. *Desarrollo normativo.*

1. El Gobierno, a propuesta del Ministro del Interior, dictará las disposiciones reglamentarias que sean precisas para el desarrollo y ejecución de lo dispuesto en esta ley, y concretamente para determinar:

a) Los requisitos y características que han de reunir las empresas y entidades objeto de regulación.

b) Las condiciones que deben cumplirse en la realización de actividades de seguridad privada y en la prestación de servicios de esta naturaleza.

c) Las características que han de reunir las medidas de seguridad privada y los medios técnicos y materiales utilizados en las actividades y servicios de seguridad privada.

d) Las funciones, deberes, responsabilidades y cualificación del personal de seguridad privada y del personal acreditado.

e) El régimen de habilitación y acreditación de dicho personal.

f) Los órganos del Ministerio del Interior competentes, en cada caso, para el desempeño de las distintas funciones.

2. Se faculta, asimismo, al Gobierno para actualizar la cuantía de las multas, de acuerdo con las variaciones del indicador público de renta de efectos múltiples.

Disposición final cuarta. *Entrada en vigor.*

Esta ley entrará en vigor a los dos meses de su publicación en el «Boletín Oficial del Estado».

§ 28

Real Decreto 2364/1994, de 9 de diciembre, por el que se aprueba el Reglamento de Seguridad Privada

Ministerio de Justicia e Interior
«BOE» núm. 8, de 10 de enero de 1995
Última modificación: 5 de abril de 2014
Referencia: BOE-A-1995-608

A partir del 5 de junio de 2014, esta norma mantiene su vigencia en lo que no contravenga a la Ley 5/2014, de 4 de abril, según establece la disposición derogatoria única de la citada Ley. Ref. BOE-A-2014-3649.
Téngase en cuenta que todas las referencias a la nacionalidad y a la residencia contenidas en este Reglamento se entenderán hechas a la nacionalidad de cualquiera de los Estados miembros de la Unión Europea y a la de los Estados parte en el Acuerdo sobre el Espacio Económico Europeo, y a la residencia en el territorio de dichos Estados, conforme establece la disposición adicional tercera del Real Decreto 1123/2001, de 19 de octubre. Ref. BOE-A-2001-21874.

La Ley 23/1992, de 30 de julio, de Seguridad Privada, en su disposición final primera, encomienda al Gobierno dictar las normas reglamentarias que sean precisas para el desarrollo y ejecución de la propia Ley. Por su parte, la disposición final cuarta de la Ley Orgánica 1/1992, de 21 de febrero, sobre Protección de la Seguridad Ciudadana, autoriza igualmente al Gobierno a dictar las normas necesarias para determinar las medidas de seguridad que, de conformidad con lo previsto en el artículo 13 del mismo texto legal, puedan ser impuestas a entidades y establecimientos.

La indudable afinidad de las materias aludidas y la finalidad idéntica de las mismas, constituida por la prevención de los delitos, aconseja desarrollarlas reglamentariamente de forma unitaria, lo que se lleva a cabo mediante el Reglamento de Seguridad Privada, que se aprueba por el presente Real Decreto.

De acuerdo con el mandato conferido por la Ley de Seguridad Privada, se determinan en el Reglamento los requisitos y características de las empresas de seguridad; las condiciones que deben cumplirse en la prestación de sus servicios y en el desarrollo de sus actividades, y las funciones, deberes y responsabilidades del personal de seguridad privada; al tiempo que se determinan los órganos competentes para el desempeño de las distintas funciones administrativas, y se abre el camino para la determinación de las características de los medios técnicos y materiales utilizables.

En relación con la determinación de las facultades que en materia de seguridad privada corresponden a las Comunidades Autónomas competentes para la protección de personas y bienes y para el mantenimiento del orden público, el Reglamento, como no podía ser menos, se limita a desarrollar lo establecido en la disposición adicional cuarta de la Ley 23/1992, de 30 de julio.

Se continúa así en este ámbito la línea favorable a una interpretación amplia de las atribuciones de las Comunidades Autónomas, en relación con la definición que de la

competencia autonómica sobre sus propios servicios policiales y sus funciones ha realizado la jurisprudencia constitucional (más concretamente la Sentencia 104/1989, de 8 de junio).

Desde esta perspectiva, el Reglamento recoge la atribución específica a las Comunidades Autónomas aludidas de funciones ejecutivas de la normativa estatal respecto a la autorización, inspección y sanción de las empresas de seguridad que tengan su domicilio social y su ámbito de actuación en la propia Comunidad Autónoma, respetando así la decisión del legislador, que entiende comprendidas, si quiera sea parcialmente, determinadas competencias sobre seguridad privada en el ámbito de las facultades autonómicas asumidas estatutariamente al amparo del artículo 149.1.29.ª de la Constitución.

En coherencia con lo anterior, la Ley 23/1992 y este Reglamento sientan de forma clara la competencia estatal respecto a aquellas actividades de seguridad privada que, por su ámbito funcional de desarrollo o por estar conectadas con aquélla, no pueden entenderse comprendidas en el ámbito de la competencia autonómica para regular su propia policía destinada al mantenimiento del orden público y a la protección de personas y bienes.

En este sentido la habilitación del personal de seguridad privada, que la Ley 23/1992 no incluyó entre las facultades autonómicas, implica el ejercicio de funciones derivadas de la competencia estatal exclusiva sobre la seguridad pública, sin que aquélla pueda incluirse en la competencia autonómica sobre sus propios servicios policiales, tal y como la define la jurisprudencia constitucional. A mayor abundamiento, se está ante una habilitación para el ejercicio de determinadas funciones en todo el territorio estatal y ante personas que en la mayor parte de los casos pueden desarrollar sus funciones provistas de armas de fuego.

Por lo que respecta a la seguridad en establecimientos e instalaciones, se desarrolla el artículo 13 de la Ley Orgánica sobre Protección de la Seguridad Ciudadana, determinando los servicios y sistemas de seguridad que habrán de adoptar las distintas clases de establecimientos, a cuyo efecto se cuenta con la experiencia acumulada durante los últimos años, adecuándose las medidas de seguridad en entidades y establecimientos públicos y privados al objeto perseguido, teniendo en cuenta las nuevas tecnologías.

Se completa así el ciclo normativo de la seguridad privada, contemplada en su totalidad, poniéndose fin a la dispersión de normas vigentes, dictadas a partir del año 1974, y subsanando las lagunas existentes y los desfases producidos por la propia dinámica de la seguridad privada durante los años transcurridos.

En su virtud, a propuesta del Ministro de Justicia e Interior, con la aprobación del Ministro para las Administraciones Públicas, oído el Consejo de Estado, y previa deliberación del Consejo de Ministros en su reunión del día 9 de diciembre de 1994,

D I S P O N G O :

Artículo único.

En desarrollo y ejecución de la Ley 23/1992, de 30 de julio, de Seguridad Privada, y del artículo 13 de la Ley Orgánica 1/1992, de 21 de febrero, sobre Protección de la Seguridad Ciudadana, se aprueba el Reglamento de Seguridad Privada, cuyo texto se inserta a continuación.

Disposición adicional primera. *Actividades excluidas.*

Quedan fuera del ámbito de aplicación del Reglamento de Seguridad Privada las actividades siguientes, realizadas por personal distinto del de seguridad privada, no integrado en empresas de seguridad, siempre que la contratación sea realizada por los titulares de los inmuebles y tenga por objeto directo alguna de las siguientes actividades:

a) Las de información en los accesos, custodia y comprobación del estado y funcionamiento de instalaciones, y de gestión auxiliar, realizadas en edificios particulares por porteros, conserjes y personal análogo.

b) En general, la comprobación y control del estado de calderas e instalaciones generales en cualesquiera clase de inmuebles, para garantizar su funcionamiento y seguridad física.

c) El control de tránsito en zonas reservadas o de circulación restringida en el interior de fábricas, plantas de producción de energía, grandes centros de proceso de datos y similares.

d) Las tareas de recepción, comprobación de visitantes y orientación de los mismos, así como las de control de entradas, documentos o carnés privados, en cualquier clase de edificios o inmuebles.

Disposición adicional segunda. *Funcionamiento del Registro General de Empresas de Seguridad.*

El Registro General de Empresas de Seguridad constituido en el Ministerio de Justicia e Interior, al que se refiere el artículo 7 de la Ley 23/1992, de 30 de julio, de Seguridad Privada, funcionará en la unidad orgánica especializada en materia de seguridad privada, dentro de la Comisaría General de Seguridad Ciudadana.

Disposición adicional tercera. *Comisiones de coordinación.*

1. Presididas por el Director general de la Policía y, en su caso, por los Gobernadores Civiles funcionarán comisiones mixtas, central y provinciales, de coordinación de la seguridad privada en el ámbito de competencias de la Administración General del Estado, integradas por representantes de las empresas y entidades obligadas a disponer de medidas de seguridad, y de los trabajadores de los sectores afectados, pudiendo integrarse en ellas asimismo representantes de las Comunidades Autónomas y de las Corporaciones Locales. La organización y funcionamiento de las comisiones serán regulados por Orden del Ministro de Justicia e Interior.

2. En las Comunidades Autónomas con competencias para la protección de las personas y bienes, y para el mantenimiento del orden público con arreglo a los correspondientes Estatutos de Autonomía y a lo previsto en la Ley Orgánica 2/1986, de Fuerzas y Cuerpos de Seguridad, también podrán existir Comisiones Mixtas de coordinación de seguridad privada en el ámbito de dichas competencias, cuya presidencia, composición y funciones sean determinadas por los órganos competentes de las mismas.

3. A las reuniones de dichas comisiones mixtas deberán ser convocados también los representantes o los jefes de seguridad de las empresas de seguridad y los representantes de los trabajadores, cuando vayan a ser tratados temas que afecten a sus servicios o actividades.

4. La convocatoria de las reuniones corresponderá efectuarla a los presidentes de las comisiones, por propia iniciativa o teniendo en cuenta las peticiones de los representantes de las empresas y de los trabajadores.

5. El régimen jurídico de estas comisiones se ajustará a las normas contenidas en el capítulo II del título II, de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, sin perjuicio de las peculiaridades organizativas que procedan en cada caso.

Disposición adicional cuarta. *Incompatibilidades del personal.*

En aplicación de lo dispuesto en los artículos 1.3 y 11.2 de la Ley 53/1984, de incompatibilidades del personal al servicio de las Administraciones Públicas, el desempeño de puestos de trabajo en dichas Administraciones por el personal incluido en el ámbito de aplicación de dicha Ley será incompatible con el ejercicio de las siguientes actividades:

a) El desarrollo de funciones propias del personal de seguridad privada.

b) La pertenencia a Consejos de Administración u órganos rectores de empresas de seguridad.

c) El desempeño de puestos de cualquier clase en empresas de seguridad.

Disposición adicional quinta. *Exclusión de las empresas relacionadas con equipos técnicos de seguridad.*

1. De conformidad con lo dispuesto en la disposición adicional sexta de la Ley 23/1992, de 30 de julio, de Seguridad Privada, introducida por la Ley 25/2009, de 22 de diciembre, los prestadores de servicios o las filiales de las empresas de seguridad privada que vendan, entreguen, instalen o mantengan equipos técnicos de seguridad, siempre que no incluyan la prestación de servicios de conexión con centrales de alarmas, quedan excluidos de la

legislación de seguridad privada, siempre y cuando no se dediquen a ninguno de los otros fines definidos en el artículo 5 de la Ley 23/1992, de 30 de julio, y sin perjuicio de otras legislaciones específicas que pudieran resultar de aplicación.

2. Las empresas de seguridad privada que, además de dedicarse a una o a varias de las actividades contempladas en el artículo 5 de la Ley 23/1992, de 30 de julio, se dediquen a la instalación de aparatos, dispositivos y sistemas de seguridad que no incluyan la conexión a centrales de alarma, sólo estarán sometidas a la legislación de seguridad privada en lo que se refiere a la prestación de las actividades y servicios regulados en el citado artículo, quedando la actividad de instalación y mantenimiento de aparatos, dispositivos y sistemas de seguridad no conectados a centrales de alarma sometida a las reglamentaciones técnicas que le sean de aplicación, y en particular a la normativa aplicable en materia de homologación de productos.

Disposición transitoria primera. *Plazo de adaptación a la Ley.*

El plazo de un año concedido por la disposición transitoria primera de la Ley 23/1992, de 30 de julio, para la adaptación a los requisitos o exigencias establecidos en la propia Ley y en sus normas de desarrollo, se contará:

a) Con carácter general, respecto a los requisitos nuevos de las empresas necesitados de concreción reglamentaria, y a las medidas de seguridad adoptadas con anterioridad, a partir de la fecha de promulgación del Reglamento de Seguridad Privada.

b) Respecto al material o equipo y a aquellas materias que, con arreglo a lo dispuesto en el mencionado Reglamento, requieran concreciones, determinaciones o aprobaciones complementarias por parte del Ministerio de Justicia e Interior, desde la fecha en que entren en vigor las correspondientes Ordenes de regulación o Resoluciones de homologación ministeriales.

c) Respecto a las materias no comprendidas en los párrafos anteriores, desde la fecha de promulgación de la Ley.

Disposición transitoria segunda. *Efectos de la adaptación y de la no adaptación.*

1. Las empresas de seguridad inscritas en el Registro, que se adapten a lo previsto en la Ley y en el Reglamento de Seguridad Privada, podrán conservar el mismo número de inscripción que tuvieren anteriormente.

2. Transcurrido el plazo de un año desde la promulgación del Reglamento de Seguridad Privada, otorgado a las empresas a efectos de adecuación a los requisitos establecidos para su inscripción en el Registro de empresas, a las que no lo hubieren hecho dentro del indicado plazo se las considerará dadas de baja en dicho Registro, estimándose cancelada su inscripción, lo que se notificará formalmente a las empresas interesadas.

Disposición transitoria tercera. *Adaptación de empresas de seguridad no inscritas anteriormente.*

1. También dispondrán del plazo de un año, contado en la forma prevista en los apartados a) y b) de la disposición transitoria primera, para adaptarse a los requisitos o exigencias propios de las empresas de seguridad establecidos en la Ley de Seguridad Privada, en el Reglamento de dicha Ley y en sus normas de desarrollo, todas aquellas empresas no inscritas en el Registro de Empresas de Seguridad, dedicadas al transporte y distribución de explosivos o a otras ramas de actividad económica y que, con anterioridad a la entrada en vigor de la Ley y con arreglo a las normas entonces vigentes, hubieran venido prestando a terceros los servicios atribuidos por la Ley de Seguridad Privada, con carácter exclusivo, a las empresas de seguridad.

2. Mientras estuvieran realizando los trámites de adaptación durante el plazo indicado, las referidas empresas tendrán la consideración de empresas de seguridad, a efectos de lo dispuesto en el artículo 12.1 de la Ley de Seguridad Privada, en relación con los vigilantes jurados de seguridad, los guardas jurados de explosivos y demás personal de seguridad privada que se encuentren prestando servicio en las mismas y lo hubieran estado prestando en la fecha de entrada en vigor de la Ley.

Disposición transitoria cuarta. *Cómputo de capital y reservas.*

A efectos de integrar los distintos niveles de recursos propios exigidos por el Reglamento de Seguridad Privada, las empresas de seguridad constituidas con anterioridad a la promulgación de la Ley 23/1992 podrán computar, además de su capital social, las reservas efectivas y expresas que consten en el balance cerrado el 31 de diciembre de 1992 y debidamente aprobado por el órgano social competente.

Disposición transitoria quinta. *Plazos de adecuación de medidas de seguridad.*

1. Sin perjuicio de lo dispuesto con carácter general en la disposición transitoria primera de la Ley 23/1992, de 30 de julio, las medidas y sistemas de seguridad instalados antes de la fecha de entrada en vigor del Reglamento de dicha Ley o de las normas que lo desarrollen, se adecuarán a los requisitos que establezcan, una vez transcurridos los siguientes plazos, a partir de aquella fecha:

A. Medidas de seguridad físicas.

a) Empresas de seguridad:

1.º Un año para instalar, en la sede social y en las delegaciones de las empresas que se dediquen a la instalación y mantenimiento de aparatos, dispositivos y sistemas de seguridad, la zona de seguridad destinada a garantizar la custodia de la información que manejaren.

2.º Un año para que las empresas de centrales de alarmas adecuen el acristalamiento de sus centros de control a los niveles de seguridad que se determinen por el Ministerio de Justicia e Interior.

b) Empresas, entidades y establecimientos obligados a la adopción de medidas de seguridad:

1.º Cinco años para instalar la puerta blindada a que se refiere el artículo 127.1.d) del Reglamento de Seguridad Privada.

2.º Cinco años para las medidas correspondientes a cámaras acorazadas y cámaras de cajas de alquiler.

No será necesaria la adecuación exigida en esta disposición transitoria a los requisitos establecidos por las normas de desarrollo del Reglamento de Seguridad Privada, de las cámaras acorazadas de efectivo que tengan por finalidad exclusiva la de proteger el encaje diario necesario para el funcionamiento de la oficina correspondiente. También será necesaria la adecuación de los compartimentos de alquiler de las cámaras, ni la de las cajas fuertes o armarios blindados en que se ubiquen compartimentos de alquiler.

Las cámaras acorazadas de efectivo, con excepción de las incluidas en el párrafo anterior, y las cámaras de cajas de alquiler instaladas con anterioridad a la fecha de entrada en vigor de las normas de desarrollo del Reglamento de Seguridad Privada, quedarán eximidas del cumplimiento del deber de adaptación a las medidas de seguridad establecidas, cuando los servicios policiales competentes verifiquen la imposibilidad física de llevar a cabo tal adaptación, y siempre que las citadas cámaras se doten de las medidas complementarias de carácter electrónico que se determinen."

Las medidas correspondientes a cámaras acorazadas de efectivo y cámaras de cajas de alquiler reguladas en el Reglamento de Seguridad Privada y normas que lo desarrollen, serán exigibles a aquéllas que se instalen por primera vez a partir de la fecha de entrada en vigor de las citadas normas de desarrollo.

3.º Cinco años para que las oficinas de farmacia instalen el dispositivo a que se refiere el artículo 131.1 de dicho Reglamento.

4.º Cinco años para que las Administraciones de Lotería, Despachos de Apuestas Mutuas y locales de juegos de azar se adapten a lo dispuesto en el artículo 132.1 y 2 y en el artículo 133 del Reglamento, respectivamente.

B) Sistemas de seguridad electrónicos:

1.º Un año para los instalados en empresas de seguridad.

2.º Dos años para los correspondientes a cámaras acorazadas o cámaras de cajas de alquiler.

3.º Un año para que, respecto a los instalados por empresas no homologadas y conectados con centrales de alarmas, se acredite ante éstas, mediante certificado de empresa habilitada en el Registro para este tipo de actividades, que la instalación se ajusta a lo dispuesto en los artículos 40, 42 y 43 del Reglamento. Transcurrido el plazo de un año sin que se haya presentado el certificado, la empresa de central de alarmas procederá a la desconexión del sistema.

4.º Cinco años para el resto de sistemas de seguridad electrónicos.

2. Los sistemas de seguridad físicos de los cajeros automáticos y cajas fuertes, regulados en el Reglamento de Seguridad Privada y normas que lo desarrollen, serán exigibles a aquellos que se instalen a partir del año siguiente a la fecha de su entrada en vigor.

Disposición transitoria sexta. *Plazo de incorporación de armeros.*

1. Transcurrido un plazo de un año, contado desde la fecha de entrada en vigor del Reglamento de Seguridad Privada, los lugares en los que se presten servicios de vigilantes de seguridad con armas deberán disponer de los armeros a que se refiere su artículo 25.

2. Durante dicho plazo, respecto a los lugares que no dispongan de armero, será de aplicación lo dispuesto en el artículo 82, apartado 2.

Disposición transitoria séptima. *Plazo de utilización de vehículos blindados.*

Los vehículos blindados utilizados por las empresas de transporte y distribución, cuyas características no se correspondan con las que determine el Ministerio de Justicia e Interior, podrán ser utilizados durante un plazo de un año, contado a partir de la entrada en vigor de las normas que al efecto se dicten. Transcurrido dicho plazo, todos los vehículos que se utilicen para esta actividad habrán de ajustarse a lo dispuesto en las citadas normas.

Disposición transitoria octava. *Disposiciones relativas a la habilitación del personal.*

A los efectos de cómputo de los plazos establecidos en las disposiciones transitorias tercera y cuarta de la Ley 23/1992, de 30 de julio, se considerarán disposiciones de desarrollo reglamentario relativas a la habilitación para el ejercicio de funciones de seguridad privada, además de las contenidas al respecto en el Reglamento de Seguridad Privada:

a) Las de concreción, determinación o aprobación de distintos aspectos, encomendadas expresamente en distintos preceptos al Ministerio de Justicia e Interior.

b) Las de regulación de la apertura y funcionamiento de los centros de formación y perfeccionamiento de personal de seguridad privada.

c) Las de regulación de las pruebas necesarias para la obtención de la tarjeta de identidad profesional del personal de seguridad privada.

Disposición transitoria novena. *Personal ya habilitado.*

1. Los vigilantes jurados de seguridad, guardas jurados de explosivos, guardas particulares jurados del campo, guardas de caza y guardapescas jurados marítimos que en la fecha de entrada en vigor de la Ley 23/1992 reunieran las condiciones exigibles para la prestación de los correspondientes servicios con arreglo a la regulación anterior a aquélla podrán seguir desempeñando las funciones para las que estuviesen documentados, sin necesidad de obtener la habilitación a que se refiere el artículo 10 de la citada Ley. Lo dispuesto en este apartado será en general aplicable a cualquier clase de personal que, independientemente de su denominación, viniera realizando funciones propias de personal de seguridad privada.

2. Los detectives privados que se encontrasen acreditados como tales en la fecha de promulgación de la indicada Ley podrán seguir desarrollando las mismas actividades hasta que transcurra un año desde la promulgación de las disposiciones de desarrollo y ejecución reglamentaria relativas a la habilitación para el ejercicio de la profesión de detective privado.

Disposición transitoria décima. *Canje de acreditaciones de personal.*

1. El personal a que se refiere la disposición transitoria anterior, que en la fecha de entrada en vigor de la Orden de aprobación de los modelos de tarjetas de identidad profesional continúe reuniendo las condiciones exigibles para la prestación de los correspondientes servicios, deberá canjear a partir de dicha fecha sus títulos-nombramientos, licencias, tarjetas de identidad o acreditaciones, por las indicadas tarjetas de identidad profesional, en los siguientes plazos:

a) Dos años, el personal mencionado en el apartado 1 de la disposición transitoria anterior.
b) Un año, los detectives privados.

2. Los jefes de seguridad que en la fecha citada en el apartado anterior se hallasen desempeñando sus funciones, con la conformidad de la Dirección de la Seguridad del Estado o del órgano competente del Ministerio de Justicia e Interior, deberán canjear su acreditación en el plazo de dos años, contado a partir de la indicada fecha.
3. Las nuevas acreditaciones se expedirán al personal mencionado, con carácter gratuito.

Disposición transitoria undécima. *Auxiliares de detectives acreditados.*

1. Los auxiliares de detective que se encontrasen acreditados como tales en la fecha de promulgación de la Ley 23/1992 podrán seguir desarrollando las mismas actividades hasta que transcurra un año desde la promulgación de las disposiciones de desarrollo y ejecución reglamentaria relativas a la habilitación para el ejercicio de la profesión de detective privado, durante cuyo plazo habrán de figurar en el Registro especial regulado en el artículo 104 del Reglamento de dicha Ley.
2. Para poder ejercer las actividades previstas en el artículo 19.1 de la citada Ley, habrán de superar durante el expresado plazo las pruebas de aptitud técnico-profesional que establezca el Ministerio de Justicia e Interior y que estarán a un nivel concordante con la titulación académica exigida para el ejercicio de las indicadas actividades, lo que les habilitará para poder obtener la tarjeta de identidad profesional de detective privado.

Disposición transitoria duodécima. *Investigadores o informadores en ejercicio.*

1. Los investigadores o informadores que acrediten oficialmente el ejercicio profesional durante dos años con anterioridad a la fecha de promulgación de la Ley 23/1992, podrán seguir desarrollando las mismas actividades hasta que transcurra un año desde la promulgación de las disposiciones de desarrollo y ejecución reglamentaria relativas a la habilitación para el ejercicio de la profesión de detective privado.
2. Para poder ejercer las actividades previstas en el artículo 19.1 de la citada Ley, habrán de superar, durante el expresado plazo, las pruebas de aptitud técnico-profesional que establezca el Ministerio de Justicia e Interior, teniendo en cuenta la experiencia obtenida en el desarrollo anterior de sus funciones, lo que les habilitará para poder obtener la tarjeta de identidad profesional de detective privado.

Disposición transitoria decimotercera. *Uniformidad del personal.*

Los vigilantes de seguridad y los guardas particulares del campo, en sus distintas modalidades, podrán seguir utilizando la uniformidad que tuvieran autorizada con anterioridad, hasta que transcurra el plazo de dos años siguiente a la fecha de entrada en vigor de las normas que dicte el Ministerio de Justicia e interior al respecto, debiendo regirse por ellas finalizado dicho plazo.

Disposición transitoria decimocuarta. *Libros-Registros abiertos.*

Las empresas de seguridad y los detectives privados podrán seguir utilizando los Libros-Registros que tuvieren abiertos, hasta que transcurra el plazo de un año, a partir de la publicación de los nuevos modelos que se aprueben con arreglo a lo dispuesto en el

Reglamento de Seguridad Privada. Finalizado dicho plazo, los Libros-Registros deberán ser sustituidos por los previstos en el Reglamento.

Disposición derogatoria única. *Alcance de la derogación normativa.*

1. Quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en el presente Real Decreto así como en el Reglamento que por el mismo se aprueba y especialmente:

a) El Real Decreto 880/1981, de 8 de mayo, sobre prestación privada de servicios de seguridad.
b) El Real Decreto 629/1978, de 10 de marzo, por el que se regula la función de los vigilantes jurados de seguridad, modificado por Real Decreto 738/1983, de 23 de febrero.
c) El Real Decreto 760/1983, de 30 de marzo, por el que se regula el nombramiento y ejercicio de las funciones de los guardas jurados de explosivos.
d) El Real Decreto de 8 de noviembre de 1849, por el que se reglamentan, entre otros, los nombramientos y funciones de los guardas particulares del campo.
e) Los apartados 2, 3 y 4 del artículo 44 del Reglamento de ejecución de la Ley de Caza, aprobado por Decreto 506/1971, de 25 de marzo.
f) El Decreto 1583/1974, de 25 de abril, por el que se aprueba el Reglamento de guardapescas jurados marítimos de establecimientos de acuicultura.
g) El Real Decreto 1338/1984, de 4 de julio, sobre Medidas de Seguridad en entidades y establecimientos públicos y privados.
h) La Orden del Ministerio del Interior, de 20 de enero de 1981, por la que se regula la profesión de detective privado.

2. No obstante lo dispuesto en el apartado anterior, permanecerán en vigor las normas sobre habilitación o nombramiento del personal de seguridad privada, hasta el momento que se determine por las normas y actos de ejecución y desarrollo del Reglamento de Seguridad Privada en el que pueda tener efectividad el sistema de formación y habilitación de dicho personal, regulado en dicho Reglamento y en los aludidos normas y actos.
3. Asimismo, seguirán exigiéndose las especificaciones o requisitos de carácter técnico, previstos en la legislación vigente, hasta que entren en vigor las correspondientes normas de desarrollo del Reglamento de Seguridad Privada.

Disposición final primera. *Disposiciones de ejecución.*

Se autoriza al Ministro de Justicia e Interior y al Ministro de Industria y Energía, previo informe, en su caso, del Ministro de Agricultura, Pesca y Alimentación y de las Comunidades Autónomas con competencias en materia de seguridad privada, para dictar, en la esfera de sus respectivas competencias, las disposiciones que sean necesarias para la ejecución y aplicación de lo dispuesto en el presente Real Decreto y en el Reglamento de Seguridad Privada.

Disposición final segunda. *Entrada en vigor.*

El presente Real Decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

REGLAMENTO DE SEGURIDAD PRIVADA

TITULO I

Empresas de Seguridad

CAPITULO I

Inscripción y autorización

Artículo 1. *Servicios y actividades de seguridad privada.*

1. Las empresas de seguridad únicamente podrán prestar o desarrollar los siguientes servicios y actividades:

a) Vigilancia y protección de bienes, establecimientos, espectáculos, certámenes o convenciones.
b) Protección de personas determinadas, previa la autorización correspondiente.
c) Depósito, custodia, recuento y clasificación de monedas y billetes, títulos-valores y demás objetos que, por su valor económico y expectativas que generen o por su peligrosidad, puedan requerir protección especial, sin perjuicio de las actividades propias de las entidades financieras.
d) Transporte y distribución de los objetos a que se refiere el apartado anterior, a través de los distintos medios, realizándolos, en su caso, mediante vehículos cuyas características serán determinadas por el Ministerio de Justicia e Interior, de forma que no puedan confundirse con los de las Fuerzas Armadas ni con los de las Fuerzas y Cuerpos de Seguridad.
e) Instalación y mantenimiento de aparatos, dispositivos y sistemas de seguridad conectados a centrales de alarma.
f) Explotación de centrales para la recepción, verificación y transmisión de las señales de alarmas y su comunicación a las Fuerzas y Cuerpos de Seguridad, así como prestación de servicios de respuesta cuya realización no sea de la competencia de dichas Fuerzas y Cuerpos.
g) Planificación y asesoramiento de las actividades de seguridad (artículo 5.1 de la Ley de Seguridad Privada).

2. Dentro de lo dispuesto en los párrafos c) y d) del apartado anterior, se comprenden la custodia, los transportes y la distribución de explosivos, sin perjuicio de las actividades propias de las empresas fabricantes, comercializadoras y consumidoras de dichos productos.
3. Las empresas de seguridad no podrán dedicarse a la fabricación de material de seguridad, salvo para su propia utilización, explotación y consumo, ni a la comercialización de dicho material. Y las empresas dedicadas a estas actividades no podrán usar, como denominación o calificativo de su naturaleza, la expresión «Empresa de Seguridad».
4. Son de carácter privado las empresas, el personal y los servicios de seguridad objeto del presente Reglamento, cuyas actividades tienen la consideración legal de actividades complementarias y subordinadas respecto a las de seguridad pública.

Artículo 2. *Obligatoriedad de la inscripción y de la autorización o reconocimiento.*

1. Para la prestación de los servicios y el ejercicio de las actividades enumerados en el artículo anterior, las empresas deberán reunir los requisitos determinados en el artículo 7 de la Ley 23/1992, de 30 de julio, de Seguridad Privada, ser autorizadas siguiendo el procedimiento regulado en los artículos 4 y siguientes de este reglamento y hallarse inscritas en el Registro de Empresas de Seguridad existente en el Ministerio del Interior.
2. Las empresas de seguridad autorizadas para la prestación de servicios de seguridad privada con arreglo a la normativa de cualquiera de los Estados miembros de la Unión Europea o de los Estados parte en el Acuerdo sobre el Espacio Económico Europeo, serán reconocidas e inscritas en el citado Registro una vez que acrediten su condición de empresa

de seguridad y el cumplimiento de los requisitos establecidos en los artículos 5, 6 y 7 de este reglamento. A tal efecto, se tendrán en cuenta los requisitos ya acreditados en cualquiera de dichos Estados y, en consecuencia, no será necesaria nueva cumplimentación de los mismos.

3. En el Registro, con el número de orden de inscripción y autorización de la empresa, figurará su denominación, número de identificación fiscal, fecha de autorización, domicilio, clase de sociedad o forma jurídica, actividades para las que ha sido autorizada, ámbito territorial de actuación y representante legal, así como las modificaciones o actualizaciones de los datos enumerados.

Artículo 3. *Ambito territorial de actuación.*

Las empresas de seguridad limitarán su actuación al ámbito geográfico, estatal o autonómico, para el que se inscriban en el Registro.

Artículo 4. *Procedimiento de autorización.*

1. El procedimiento de autorización constará de tres fases, que requerirán documentaciones específicas y serán objeto de actuaciones y resoluciones sucesivas, considerándose únicamente habilitadas de forma definitiva las empresas de seguridad cuando obtengan la autorización de entrada en funcionamiento.

2. No obstante lo dispuesto en el apartado anterior, a petición de la empresa interesada podrán desarrollarse de forma conjunta, sin solución de continuidad, la primera y la segunda de las fases indicadas, e incluso la totalidad del procedimiento de autorización.

En este caso, junto a la solicitud deberá acompañarse la documentación correspondiente a las diferentes fases parar las que se solicite la tramitación conjunta.

Artículo 5. *Documentación.*

1. El procedimiento de autorización se iniciará a solicitud de la sociedad o persona interesada, que deberá acompañar los siguientes documentos:

a) Fase inicial, de presentación:

1.º Si se trata de sociedades, copia auténtica de la escritura pública de constitución, en la que deberá constar que la sede social o establecimiento se encuentra en un Estado miembro de la Unión Europea o de un Estado parte en el Acuerdo sobre el Espacio Económico Europeo, su objeto social, que habrá de ser exclusivo y coincidente con uno o más de los servicios o actividades a que se refiere el artículo 1 de este reglamento, titularidad del capital social, y certificado de la inscripción o nota de inscripción reglamentaria de la sociedad en el Registro Mercantil o, en su caso, en el Registro de Cooperativas que corresponda, o documento equivalente en el caso de sociedades constituidas en cualquiera de dichos Estados.

2.º Declaración de la clase de actividades que pretende desarrollar y ámbito territorial de actuación.

No podrá inscribirse en el Registro ninguna empresa cuya denominación induzca a error con la de otra ya inscrita o con la de órganos o dependencias de las Administraciones Públicas, pudiendo formularse consultas previas al Registro, para evitar tal error.

b) Segunda fase, de documentación de requisitos previos:

1.º Inventario de los medios materiales de que disponga para el ejercicio de sus actividades.

2.º Documento acreditativo del título en virtud del cual dispone de los inmuebles en que se encuentre el domicilio social y demás locales de la empresa, cuando aquéllos estén ubicados en España.

3.º Si se trata de sociedades, composición personal de los órganos de administración y dirección.

c) Tercera fase, de documentación complementaria y resolución:

1.º En su caso, certificado de inscripción de la escritura pública de constitución de la sociedad en el Registro Mercantil, o en el Registro de Cooperativas correspondiente o documento equivalente, si no se hubiera presentado con anterioridad.

2.º Certificado acreditativo de la instalación de un sistema de seguridad, de las características que determine el Ministerio del Interior.

3.º Documento acreditativo del alta en el Impuesto de Actividades Económicas.

4.º Memoria explicativa de los planes de operaciones a que hayan de ajustarse las diversas actividades que pretenden realizar.

5.º Relación del personal, con expresión de su categoría y del número del documento nacional de identidad, o, en el caso de nacionales de Estados miembros de la Unión Europea o de Estados parte en el Acuerdo sobre el Espacio Económico Europeo, del número de identidad de extranjero. Cuando no haya obligación de obtener este último, se expresará el número del documento de identidad equivalente.

6.º Documentación acreditativa de las suscripción de un contrato de seguro de responsabilidad civil, aval u otra garantía financiera contratada con entidad debidamente autorizada de cualquiera de los Estados miembros de la Unión Europea o de Estados parte en el Acuerdo sobre el Espacio Económico Europeo, con el objeto de cubrir, hasta la cuantía de los límites establecidos en el anexo del presente reglamento, la responsabilidad civil que por los daños en las personas o los bienes pudieran derivarse de la explotación de la actividad o actividades para las que la empresa esté autorizada.

A las empresas legalmente autorizadas en otro Estado miembro de la Unión Europea o en un Estado parte en el Acuerdo sobre el Espacio Económico Europeo para ejercer actividades o prestar servicios de seguridad privada en dicho Estado y que pretendan ejercer tales actividades o servicios en España, se les tendrá en cuenta el contrato de seguro de responsabilidad civil, aval u otra garantía financiera, que hubieran suscrito a los mismos efectos en cualquiera de dichos Estados, siempre que el mismo cumpla los requisitos establecidos en este apartado.

Si el seguro de responsabilidad civil, aval u otra garantía financiera suscrito en cualquiera de los Estados miembros de la Unión Europea o de un Estado parte en el Acuerdo sobre el Espacio Económico Europeo lo fuese por cuantía inferior a la exigida a las empresas españolas por la vigente normativa de seguridad privada, la empresa obligada a su prestación deberá constituir nuevo seguro, aval o garantía complementarios o ampliar el ya suscrito hasta alcanzar dicha cuantía.

7.º Documentación acreditativa de haber constituido garantía, en la forma y condiciones prevenidas en el artículo 7 de este reglamento.

2. Los documentos prevenidos en los apartados anteriores se presentarán adaptados para acreditar el cumplimiento de los requisitos específicos que para cada tipo de actividad se exigen a las empresas de seguridad, con arreglo a lo dispuesto en el anexo de este reglamento.

3. Sin perjuicio de las funciones de inspección y control que corresponden a la Dirección General de la Policía y de la Guardia Civil (ámbito del Cuerpo Nacional de Policía) en materia de seguridad privada, el preceptivo informe del Cuerpo de la Guardia Civil sobre idoneidad de instalación de los armeros que, en su caso, hayan de tener las empresas de seguridad, deberá ser emitido a instancia del Cuerpo Nacional de Policía e incorporado oportunamente al expediente de inscripción.

Artículo 6. *Habilitación múltiple.*

Las empresas que pretendan dedicarse a más de una de las actividades o servicios enumerados en el artículo 1 de este reglamento, habrán de acreditar los requisitos generales, así como los específicos que pudieran afectarles, con las siguientes peculiaridades:

a) El que se refiere a Jefe de Seguridad, que podrá ser único para las distintas actividades.

b) Los relativos a póliza de responsabilidad civil, aval u otra garantía financiera con entidad debidamente autorizada, y a la garantía a la que se refiere el artículo 7 de este reglamento: Si van a realizar dos actividades o servicios, justificarán la mayor de las

cantidades exigidas por cada uno de los dos conceptos. Si pretenden realizar más de dos actividades, la correspondiente póliza de responsabilidad civil, aval u otra garantía financiera, y la garantía regulada en el artículo 7, se incrementarán en una cantidad igual al 25 por ciento de las exigidas para cada una de las restantes clases de servicios o actividades.

Artículo 7. *Constitución de garantía.*

1. Las empresas de seguridad habrán de constituir una garantía en la Caja General de Depósitos o en organismo de naturaleza similar de cualquier Estado miembro de la Unión Europea o Estado parte en el Acuerdo sobre el Espacio Económico Europeo, a disposición de las autoridades con competencias sancionadoras en la materia, con el fin de atender a las responsabilidades que deriven del funcionamiento de la empresas por infracciones a la normativa de seguridad privada.

2. En el caso de que la garantía se constituya en la Caja General de Depósitos, se hará en alguna de las modalidades previstas en la normativa reguladora de dicho organismo, con los requisitos establecidos en la misma.

3. La garantía deberá mantenerse por la cuantía máxima de su importe durante todo el período de vigencia de la autorización, con cuya finalidad las cantidades que, en su caso, se hubieren detraído a los efectos previstos en el apartado 1 de este artículo habrán de reponerse en el plazo de un mes a contar desde la fecha en que hubieren ejecutado los correspondientes actos de disposición.

4. Las empresas legalmente autorizadas en otro Estado miembro de la Unión Europea o en un Estado parte en el Acuerdo sobre el Espacio Económico Europeo para ejercer actividades o prestar servicios de seguridad privada en dicho Estado y que pretendan ejercer tales actividades o servicios en España, podrán constituir la garantía a que se refieren los apartados anteriores en los organismos o entidades autorizados para ello de cualquiera de dichos Estados, siempre que la misma se encuentre a disposición de las autoridades españolas para atender a las responsabilidades que deriven del funcionamiento de la empresa por infracciones a la normativa de seguridad privada.

A las empresas a las que se refiere el párrafo anterior, se les tendrá en cuenta la garantía que, en su caso, hubieran suscrito a los mismos efectos en cualquier Estado miembro de la Unión Europea o parte en el Acuerdo sobre el Espacio Económico Europeo, siempre que cumpla los requisitos mencionados en los apartados anteriores y su cuantía sea equivalente a la exigida a las empresas españolas en virtud de lo dispuesto en el anexo de este reglamento.

Si la garantía depositada en cualquiera de dichos Estados fuese de cuantía inferior a la exigida a las empresas españolas por la vigente normativa de seguridad privada, la empresa depositante deberá constituir nueva garantía complementaria o ampliar la ya suscrita hasta alcanzar dicha cuantía.

Artículo 8. *Subsanación de defectos.*

Si la solicitud inicial, o las que inicien las fases sucesivas cuando el procedimiento conste de dos o tres fases, fueran defectuosas o incompletas, se requerirá al solicitante para que subsane la falta o acompañe los documentos preceptivos, con apercibimiento de que, en caso contrario y una vez transcurridos diez días sin cumplimentar el requerimiento, se le tendrá por desistido y se archivará el expediente.

Artículo 9. *Resoluciones y recursos.*

1. La Administración actuante resolverá motivadamente las distintas fases del procedimiento dentro del plazo de dos meses a partir de la fecha de entrada de la solicitud en cualquiera de los registros del órgano administrativo competente, notificándose a la persona o entidad interesada, con especificación, respecto a la inscripción y autorización, de la actividad o actividades que pueden desarrollar, ámbito territorial de actuación y número de inscripción y autorización asignado.

2. Cuando, dentro del mismo plazo de dos meses determinado en el apartado anterior, se entendiese en cualquiera de las fases del procedimiento que la empresa no reúne los

requisitos necesarios, se resolverá denegando la solicitud, con indicación de los recursos que pueden utilizarse contra la denegación.

3. No obstante lo dispuesto en el apartado anterior, si venciese el plazo de resolución y el órgano competente no la hubiese dictado expresamente, podrá entenderse desestimada la solicitud, pudiendo el interesado interponer contra dicha desestimación presunta los recursos procedentes.

Artículo 10. *Coordinación registral.*

1. El Registro establecido en el Ministerio de Justicia e Interior constituirá el Registro General de Empresas de Seguridad, al cual, aparte de la información correspondiente a las empresas que en el mismo se inscriban, se incorporará la relativa a las empresas inscritas en los registros de las Comunidades Autónomas con competencia en la materia.

2. A efectos de lo dispuesto en el apartado anterior, los órganos competentes de las mencionadas Comunidades Autónomas deberán remitir oportunamente al Registro General de empresas de seguridad copia de las inscripciones y anotaciones que efectúen sobre las empresas de seguridad que inscriban y autoricen, así como de sus modificaciones y cancelación.

3. Toda la información y documentación incorporadas al Registro General de Empresas de Seguridad estará a disposición de los órganos competentes de las Comunidades Autónomas para el ejercicio de sus funciones en materia de seguridad privada.

4. Los sistemas de numeración de los Registros, General y Autonómicos, de empresas de seguridad se determinarán coordinadamente, de forma que el número de inscripción de una empresa de seguridad no pueda coincidir con el de ninguna otra.

CAPITULO II

Modificaciones de inscripción y cancelación

Sección 1.ª Modificaciones de inscripción

Artículo 11. *Supuestos de modificación.*

1. Cualquier variación de los datos incorporados al Registro de empresas de seguridad, enumerados en el artículo 2.3 de este Reglamento, deberá ser objeto del correspondiente expediente de modificación.

2. Las empresas de seguridad podrán solicitar las modificaciones de su inscripción referidas a dichos datos, y en especial a la ampliación o reducción de actividades o de ámbito territorial de actuación.

3. En cualquiera de los supuestos de modificación, los requisitos necesarios, la documentación a aportar y la tramitación del procedimiento deberán atenerse a lo dispuesto en el capítulo anterior y en el anexo de este Reglamento.

4. Si en el momento de la solicitud o durante la tramitación de la misma, a la empresa se le siguiera expediente administrativo por pérdida de los requisitos, recursos humanos o medios materiales o técnicos que permitieron la inscripción o autorización, los dos procedimientos serán objeto de acumulación y de resolución conjunta.

Sección 2.ª Cancelación

Artículo 12. *Causas de cancelación.*

1. Los requisitos, recursos humanos y medios materiales y técnicos exigidos para la inscripción y autorización de las empresas de seguridad deberán mantenerse durante todo el tiempo de vigencia de la autorización.

2. La inscripción de empresas de seguridad para el ejercicio de las actividades o la prestación de servicios a que se refiere el artículo 1 de este Reglamento se cancelará, por el Ministro de Justicia e Interior, por las siguientes causas:

a) Petición propia.

b) Pérdida de alguno de los requisitos, recursos humanos y medios materiales o técnicos exigidos en el capítulo anterior y en el anexo del presente Reglamento.

c) Cumplimiento de la sanción de cancelación.

d) Inactividad de la empresa de seguridad durante el plazo de un año.

Artículo 13. *Efectos de la cancelación.*

1. La cancelación de la inscripción de empresas de seguridad determinará la liberación de la garantía regulada en el artículo 7 de este reglamento, una vez atendidas las responsabilidades a que se refiere el apartado 1 de dicho artículo.

2. No se podrá efectuar la liberación de la garantía cuando la empresa tenga obligaciones económicas pendientes con la Administración derivadas del funcionamiento de la empresa por infracciones a la normativa de seguridad privada, o cuando se le instruya expediente sancionador, hasta su resolución y, en su caso, hasta el cumplimiento de la sanción.

3. No obstante, podrá reducirse la garantía, teniendo en cuenta el alcance previsible de las obligaciones y responsabilidades pendientes.

4. En el supuesto de cancelación por inactividad, la reanudación de la actividad requerirá la instrucción y resolución de un nuevo procedimiento de autorización.

CAPITULO III

Funcionamiento

Sección 1.ª Disposiciones comunes

Artículo 14. *Obligaciones generales.*

1. En el desarrollo de sus actividades, las empresas de seguridad vienen obligadas al especial auxilio y colaboración con las Fuerzas y Cuerpos de Seguridad. A estos efectos deberán comunicar a dichas Fuerzas y Cuerpos cualesquiera circunstancias e informaciones relevantes para la prevención, el mantenimiento o el restablecimiento de la seguridad ciudadana, así como los hechos delictivos de que tuvieren conocimiento en el desarrollo de dichas actividades.

Las empresas de seguridad deberán comunicar las altas y bajas del personal de seguridad privada de que dispongan a las dependencias correspondientes de las Fuerzas y Cuerpos de Seguridad, dentro del plazo de cinco días siguientes a la fecha en que se produzcan.

2. Deberá realizarse siempre con las debidas garantías de seguridad y reserva la prestación de los servicios de protección de personas, depósito, custodia y tratamiento de objetos valiosos, y especialmente los relativos a transporte y distribución de objetos valiosos y de explosivos u otros objetos peligrosos, en lo que respecta a su programación así como a su itinerario.

3. Los servicios y actividades de seguridad deberán ser realizados directamente por el personal de la empresa contratada para su prestación, no pudiendo ésta subcontratarlos con terceros, salvo que lo haga con empresas inscritas en los correspondientes Registros y autorizadas para la prestación de los servicios o actividades objeto de subcontratación, y se cumplan los mismos requisitos y procedimientos prevenidos en este Reglamento para la contratación. La subcontratación no producirá exoneración de responsabilidad de la empresa contratante.

4. No será exigible el requisito de identidad de dedicación, en el supuesto de subcontratación con empresas de vigilancia y protección de bienes, previsto en el artículo 49.4.

Artículo 15. *Comienzo de actividades.*

Una vez inscritas y autorizadas, y antes de entrar en funcionamiento las empresas de seguridad habrán de comunicar la fecha de comienzo de sus actividades a la Dirección General de la Policía, que informará a los Gobiernos Civiles y a las dependencias periféricas

de la misma o a las de la Dirección General de la Guardia Civil del lugar en que radiquen. Las empresas que se dediquen a la explotación de centrales de alarmas, deberán dar cuenta, además, de las fechas de efectividad de las distintas conexiones a las dependencias policiales a las que corresponda dar respuesta a las alarmas.

Artículo 16. *Publicidad de las empresas.*

1. El número de orden de inscripción en el Registro que le corresponda a cada empresa deberá figurar en los documentos que utilice y en la publicidad que desarrolle.

2. Ninguna empresa podrá realizar publicidad relativa a cualquiera de las actividades y servicios a que

hace referencia el artículo 1 de este Reglamento, sin hallarse previamente inscrita en el Registro y autorizada para entrar en funcionamiento.

Artículo 17. *Apertura de sucursales.*

1. Las empresas de seguridad que pretendan abrir delegaciones o sucursales lo solicitarán a la Dirección General de la Policía y de la Guardia Civil (ámbito del Cuerpo Nacional de Policía), acompañando los siguientes documentos:

a) Inventario de los bienes materiales que se destinan al ejercicio de las actividades en la delegación o sucursal.

b) Documento acreditativo del título en virtud del cual se dispone del inmueble o inmuebles destinados a la delegación o sucursal.

c) Relación del personal de la delegación o sucursal, con expresión de su cargo, categoría y del número del documento nacional de identidad o, en el caso de nacionales de Estados miembros de la Unión Europea o de Estados parte en el Acuerdo sobre el Espacio Económico Europeo, del número de identidad de extranjero. Cuando no haya obligación de obtener este último, se expresará el número del documento de identidad equivalente.

2. Las empresas de seguridad deberán abrir delegaciones o sucursales, dando conocimiento a la Dirección General de la Policía y de la Guardia Civil (ámbito del Cuerpo Nacional de Policía), con aportación de los documentos reseñados en el apartado anterior, en las Ciudades de Ceuta y Melilla o en las provincias en que no radique su sede principal, cuando realicen en dichas ciudades o provincias alguna de las siguientes actividades:

a) Depósito, custodia, recuento y clasificación de monedas y billetes, títulos-valores, así como custodia de objetos valiosos, explosivos u objetos peligrosos. Estas delegaciones deberán contar con los requisitos de dotación de vigilantes de seguridad, armero o caja fuerte, y cámara acorazada y locales anejos, a que se refieren los apartados 3.1.B) y 3.1.C), c) y d) del anexo para objetos valiosos y peligrosos, y con los de dotación de vigilantes de seguridad y armero o caja fuerte, a que se refieren los apartados 3.2.B) y 3.2.C), c) del anexo, respecto a explosivos.

No obstante, cuando la cantidad a custodiar por dichas delegaciones o sucursales no supere los 601.012 euros, siempre que al menos el cincuenta por ciento sea en moneda fraccionaria, la cámara acorazada podrá ser sustituida por una caja fuerte con las características determinadas por el Ministerio del Interior.

b) Vigilancia y protección de bienes y establecimientos, cuando el número de vigilantes de seguridad que presten servicio en la provincia sea superior a treinta y la duración del servicio, con arreglo al contrato o a las prórrogas de éste, sea igual o superior a un año.

3. Las empresas de seguridad autorizadas para la prestación de actividades o servicios de seguridad privada con arreglo a la normativa de cualquiera de los Estados miembros de la Unión Europea de Estados parte en el Acuerdo sobre el Espacio Económico Europeo, que hayan sido reconocidas en España con arreglo al procedimiento previsto en este real decreto, y que pretendan ejercer tales actividades o servicios en España con carácter permanente, deberán abrir delegaciones, sucursales, filiales o agencias en España.

Dichas delegaciones, sucursales, filiales o agencias deberán cumplir los requisitos previstos en el apartado 1 de este artículo y disponer de las medidas de seguridad previstas en este reglamento para las empresas de seguridad.

Artículo 18. *Características de los vehículos.*

Los vehículos utilizados por las empresas de seguridad habrán de reunir las características a que se refiere el artículo 1.d) de este Reglamento, no pudiendo disponer de lanza-destellos o sistemas acústicos destinados a obtener preferencia de paso a efectos de circulación vial.

Artículo 19. *Libros-registros.*

1. Las empresas de seguridad llevarán obligatoriamente los siguientes libros-registro:

a) Las empresas que estén obligadas a tener sistema de seguridad instalado, libro-catálogo de medidas de seguridad.

b) Libro-registro de comunicaciones a las Fuerzas y Cuerpos de Seguridad, en el que se anotarán cuantas realicen sobre aspectos relacionados con la seguridad ciudadana, fecha de cada comunicación, órgano al que se dirigió e indicación de su contenido.

2. El formato de los reseñados libros-registros se ajustará a las normas que respectivamente apruebe el Ministerio del Interior, de forma que sea posible su tratamiento y archivo mecanizado e informatizado.

3. Tanto los libros-registro de carácter general como los específicos que se determinan en este Reglamento para cada actividad se llevarán en la sede principal de la empresa y en sus delegaciones o sucursales, debiendo estar siempre a disposición de los miembros del Cuerpo Nacional de Policía y de la Policía Autónoma correspondiente, encargados de su control.

4. En ausencia del director, administrador o jefe de seguridad, los libros-registro indicados se facilitarán por el personal presente en la empresa, que habrá de estar designado al efecto, durante las inspecciones que realicen los miembros de los citados Cuerpos o Policías.

Artículo 20. *Contratos de servicio.*

1. Las empresas de seguridad comunicarán con una antelación mínima de tres días, de forma individualizada para cada servicio, la iniciación del mismo, con indicación del lugar de prestación, la clase de actividad, la persona física o jurídica contratante y su domicilio, así como la duración prevista de la vigencia del contrato.

La referida comunicación de los contratos se efectuará por cualquier medio que permita dejar constancia de ello, en la comisaría provincial o local de policía del lugar donde se celebre el contrato, o, en los lugares en que éstas no existan, en los cuarteles o puestos de la Guardia Civil, que la transmitirán o remitirán con carácter urgente a la comisaría correspondiente al lugar en que haya de prestarse el servicio ; pudiendo efectuarse en cualquier caso, en los respectivos servicios o inspecciones de guardia.

Las modificaciones de los contratos se comunicarán, en la misma forma y plazos indicados, ante las dependencias policiales mencionadas.

El formato de los contratos y de las comunicaciones se ajustará a las normas y modelos que se establezcan por el Ministerio del Interior, sin perjuicio de la posibilidad de adición en los contratos, de pactos complementarios para aspectos no regulados en el presente Reglamento.

En cualquier caso, los contratos permanecerán en las sedes de las empresas de seguridad a disposición de los órganos de las Fuerzas y Cuerpos de Seguridad competentes en materia de inspección y control, durante un plazo de cinco años desde la finalización del servicio objeto del contrato.

2. En aquellos supuestos en que los contratos se concierten con Administraciones públicas o se encuentren en tramitación ante órganos de las mismas, no siendo posible que estén formalizados antes del inicio del servicio, las empresas de seguridad deberán aportar, en su caso, con la antelación indicada en el apartado anterior, copia autorizada o declaración de la empresa de la oferta formulada, para conocimiento de las circunstancias a que se refieren las cláusulas por los órganos encargados de la inspección y control, sin perjuicio de comunicar en el formato establecido los datos del contrato una vez formalizado el mismo, el

cual deberá quedar en la sede de la empresa a disposición de los órganos competentes de las Fuerzas y Cuerpos de Seguridad.

3. Cuando circunstancias excepcionales de robo, incendio, daños, catástrofes, conflictos sociales, averías de los sistemas de seguridad u otras causas de análoga gravedad o de extraordinaria urgencia, hicieran necesaria la prestación inmediata de servicio cuya organización previa hubiera sido objetivamente imposible, se comunicarán por el procedimiento más rápido disponible, antes de comenzar la prestación de los servicios, los datos enumerados en el párrafo primero del apartado 1 de este artículo a la dependencia policial correspondiente, indicando las causas determinantes de la urgencia, y quedando obligada la empresa a formalizar el contrato dentro de las setenta y dos horas siguientes a la iniciación del servicio, debiendo permanecer el contrato en la sede de la empresa a disposición de los órganos competentes de las Fuerzas y Cuerpos de Seguridad.

Los servicios de seguridad a que se refiere el párrafo anterior podrán ser prestados con armas, dando cuenta a la dependencia policial competente, cuando los supuestos descritos se produzcan en establecimientos obligados a tener medidas de seguridad que resulten anuladas por las circunstancias expuestas, o por otras, con grave riesgo para la integridad de los bienes protegidos y teniendo en cuenta la cuantía e importancia de éstos.

Artículo 21. *Contratos con defectos.*

Cuando la comunicación, el contrato o la oferta de servicios de las empresas de seguridad no se ajusten a las exigencias prevenidas, la Subdelegación del Gobierno -que podrá delegar en la correspondiente Jefatura Superior o Comisaría Provincial de Policía- les notificará las deficiencias, con carácter urgente, a efectos de que puedan ser subsanadas en los cinco días hábiles siguientes, con apercibimiento de que, de no hacerlo en el plazo indicado, los citados documentos se archivarán sin más trámite, no pudiendo comenzar la prestación del servicio, o continuarla si ya hubiese comenzado.

Artículo 22. *Suspensión de servicios.*

(Anulado)

Sección 2.ª Empresas inscritas para actividades de vigilancia, protección de personas y bienes, depósito, transporte y distribución de objetos valiosos, explosivos u objetos peligrosos

Artículo 23. *Adecuación de los servicios a los riesgos.*

Las empresas inscritas y autorizadas para el desarrollo de las actividades a que se refieren los párrafos a), b), c) y d) del artículo 1 de este Reglamento, antes de formalizar la contratación de un servicio de seguridad, deberán determinar bajo su responsabilidad la adecuación del servicio a prestar respecto a la seguridad de las personas y bienes protegidos, así como la del personal de seguridad que haya de prestar el servicio, teniendo en cuenta los riesgos a cubrir, formulando, en consecuencia, por escrito, las indicaciones procedentes.

Artículo 24. *Comunicación entre la sede de la empresa y el personal de seguridad.*

Las empresas deberán asegurar la comunicación entre su sede y el personal que desempeñe los siguientes servicios:

a) Vigilancia y protección de polígonos industriales o urbanizaciones.
b) Transporte y distribución de objetos valiosos o peligrosos.
c) Custodia de llaves en vehículos, en servicios de respuesta a alarmas.
d) Aquellos otros que, por sus características, se determinen por el Gobierno Civil de la provincia.

Artículo 25. *Armeros.*

1. En los lugares en que se preste servicio de vigilantes de seguridad con armas o de protección de personas determinadas, salvo en aquellos supuestos en que la duración del

servicio no exceda de un mes, deberán existir armeros que habrán de estar aprobados por el Gobierno Civil de la provincia, previo informe de la correspondiente Intervención de Armas y Explosivos de la Guardia Civil, una vez comprobado que se cumplen las medidas de seguridad determinadas por la Dirección General de la Guardia Civil.

2. En dichos lugares, deberá existir un libro-registro de entrada y salida de armas, concebido de forma que sea posible su tratamiento y archivo mecanizado e informatizado, en el que se anotarán, en cada relevo que se produzca en el servicio, las armas depositadas, las armas que portan los vigilantes, y los restantes datos que se determinen en el correspondiente modelo.

3. En el domicilio social de las empresas de seguridad o en el de sus delegaciones o sucursales, según proceda, deberá estar depositada una llave de tales armeros.

4. Cuando se trate de los servicios especiales determinados en el artículo 82.2 de este Reglamento, la utilización del armero podrá sustituirse por el uso de la caja fuerte del local, custodiando el arma en una caja metálica cerrada con llave. La llave de esta caja metálica deberá estar en posesión del vigilante, y una copia depositada en el domicilio de la empresa de seguridad o en el de su delegación o sucursal.

Artículo 26. *Armas reglamentarias.*

1. Las armas reglamentarias que han de portar y utilizar los vigilantes de seguridad, escoltas privados y guardas particulares del campo, en el ejercicio de sus funciones, se adquirirán por las empresas y serán de su propiedad.

2. Para la tenencia legal de dichas armas, en número que no podrá exceder del que permitan las licencias obtenidas por el personal con arreglo al Reglamento de Armas, las empresas de seguridad habrán de solicitar y necesitarán obtener de los órganos correspondientes de la Dirección General de la Guardia Civil las guías de pertenencia de dichas armas.

3. Además de las armas que posean para la prestación de los servicios, las empresas de seguridad habrán de disponer de armas en número equivalente al 10 por 100 del de vigilantes de seguridad, al objeto de que éstos puedan realizar los ejercicios obligatorios de tiro. La Dirección General de la Guardia Civil comunicará a la de la Policía, y, en su caso, a la Policía de la correspondiente Comunidad Autónoma, el número y clases de armas que las empresas tengan en cada uno de sus locales.

4. El personal a que se refiere el apartado 1 del presente artículo realizará los ejercicios obligatorios de tiro en la fecha que se determine por las empresas de seguridad, bajo la supervisión de la Guardia Civil, de acuerdo con las instrucciones que imparta la Dirección General de dicho Cuerpo.

5. En las galerías de tiro en que se lleven a cabo los ejercicios, que habrán de encontrarse autorizadas conforme a lo previsto en el Reglamento de Armas, tanto si son propias como si son ajenas a las empresas de seguridad, los vigilantes de seguridad, escoltas privados y demás personal de seguridad privada habrán de realizar las prácticas de manejo y perfeccionamiento en el uso de armas, siempre ante la presencia y bajo la dirección del jefe de seguridad o de un instructor de tiro, ambos de competencia acreditada.

Sección 3.ª Protección de personas

Artículo 27. *Personas y empresas autorizadas.*

La actividad de protección de personas podrá ser desarrollada únicamente por escoltas privados integrados en empresas de seguridad, inscritas para el ejercicio de dicha actividad, y que habrán de obtener previamente autorización específica para cada contratación de servicio de protección, de acuerdo con lo dispuesto en los artículos siguientes.

Artículo 28. *Solicitud, tramitación y resolución.*

1. Los servicios de protección deberán ser solicitados, directamente por la persona interesada o a través de la empresa de seguridad que se pretenda encargar de prestarlos, ya sean en favor del propio interesado o de las personas que tenga bajo su guarda o custodia o de cuya seguridad fuera responsable.

2. El procedimiento se tramitará con carácter urgente, y en el mismo habrá de obtenerse el informe de la Dirección General de la Guardia Civil, cuando sea procedente, teniendo en cuenta los lugares en que haya de realizarse principalmente la actividad.

En la solicitud, que se dirigirá al Director general de la Policía, se harán constar los riesgos concretos de las personas a proteger, valorando su gravedad y probabilidad y acompañando cuantos datos o informes se consideren pertinentes para justificar la necesidad del servicio. Asimismo, cuando la autorización se solicite personalmente, se expresará en la solicitud la empresa de seguridad a la que se pretenda encargar de prestarlo.

3. La Dirección General de la Policía, considerando la naturaleza del riesgo, su gravedad y probabilidad, determinará si es necesaria la prestación del servicio de protección o si, por el contrario, es suficiente la adopción de medidas de autoprotección. Los servicios de protección personal habrán de ser autorizados, expresa e individualizadamente y con carácter excepcional, cuando, a la vista de las circunstancias expresadas resulten imprescindibles, y no puedan cubrirse por otros medios.

4. La resolución en que se acuerde la concesión o denegación de la autorización, que habrá de ser motivada, determinará el plazo de vigencia de la misma, podrá incorporar condicionamientos sobre su forma de prestación, concretará si ha de ser prestado por uno o más escoltas privados con las armas correspondientes, y se comunicará al interesado y a la empresa de seguridad.

Artículo 29. *Autorización provisional.*

Cuando con base en la solicitud e información presentada con arreglo al apartado 1 del artículo 28 resultara necesario, teniendo en cuenta las circunstancias y urgencia del caso, podrá concederse con carácter inmediato una autorización provisional para la prestación de servicios de protección personal, por el tiempo imprescindible hasta que se pueda adoptar la resolución definitiva.

Artículo 30. *Prestación y finalización del servicio.*

1. La empresa de seguridad encargada comunicará a la Dirección General de la Policía la composición del personal de la escolta, así como sus variaciones tan pronto como se produzcan, informando en su caso de los escoltas relevados, de los que les sustituyan y de las causas de la sustitución.

2. **(Derogado)**

3. Los servicios de protección de personas podrán ser prorrogados, a instancia del solicitante, cuando lo justifiquen las circunstancias que concurran.

4. La empresa de seguridad deberá comunicar a la Dirección General de la Policía la finalización del servicio, así como sus causas, en el plazo de las cuarenta y ocho horas siguientes al momento de producirse aquélla.

5. Simultáneamente a la notificación de las autorizaciones que conceda, la Dirección General de la Policía comunicará a las unidades correspondientes de las Fuerzas y Cuerpos de Seguridad del Estado las autorizaciones concedidas, los datos de las personas protegidas y de los escoltas encargados de los servicios, así como su fecha de iniciación y finalización.

Sección 4.ª Depósito y custodia de objetos valiosos o peligrosos y explosivos

Artículo 31. *Particularidades de estos servicios.*

1. En los contratos en que se concierte la prestación de servicios de depósito y custodia habrá de constar la naturaleza de los objetos que hayan de ser depositados o custodiados y, en su caso, clasificados, así como una valoración de los mismos.

2. Las empresas dedicadas a la prestación de estos servicios llevarán un libro-registro de depósitos, cuyo formato se ajustará a las normas que se aprueben por el Ministerio del Interior.

Sección 5.ª Transporte y distribución de objetos valiosos o peligrosos y explosivos

Artículo 32. *Vehículos.*

1. La prestación de los servicios de transporte y distribución de objetos valiosos o peligrosos habrá de efectuarse en vehículos blindados de las características que se determinen por el Ministerio de Justicia e Interior, cuando las cantidades, el valor o la peligrosidad de lo transportado superen los límites o reúnan las características que asimismo establezca dicho Ministerio, sin perjuicio de las competencias que corresponden al Ministerio de Industria y Energía.

Cuando las características o tamaño de los objetos, especificados por Orden del Ministerio de Justicia e Interior impidan o hagan innecesario su transporte en vehículos blindados, éste se podrá realizar en otros vehículos, contando con la debida protección en cada caso, determinada con carácter general en dicha Orden o, para cada caso concreto, por el correspondiente Gobierno Civil.

Los viajantes de joyería solamente podrán llevar consigo reproducciones de joyas u objetos preciosos cuya venta promocionen, o las piezas originales, cuando su valor en conjunto no exceda de la cantidad que determine el Ministerio de Justicia e Interior.

2. Las características de los vehículos de transporte y distribución de explosivos se determinarán teniendo en cuenta lo dispuesto en el Reglamento de Transporte de Mercancías Peligrosas (TPC), para dichas materias.

Artículo 33. *Dotación y funciones.*

1. La dotación de cada vehículo blindado estará integrada, como mínimo, por tres vigilantes de seguridad, uno de los cuales realizará exclusivamente la función de conductor.

2. Durante las operaciones de transporte, carga y descarga, el conductor se ocupará del control de los dispositivos de apertura y comunicación del vehículo, y no podrá abandonarlo; manteniendo en todo momento el motor en marcha cuando se encuentre en vías urbanas o lugares abiertos. Las labores de carga y descarga las efectuará otro vigilante, encargándose de su protección durante la operación el tercer miembro de la dotación, que portará al efecto el arma determinada de acuerdo con lo dispuesto en el artículo 86 de este Reglamento.

3. La dotación y las funciones de los vigilantes de cada vehículo de transporte y distribución de explosivos se determinarán con arreglo a lo que disponga el Reglamento de Explosivos, aprobado por el Real Decreto 230/1998, de 16 de febrero.

Artículo 34. *Hoja de ruta.*

1. Las operaciones de recogida y entrega que realice cada vehículo se consignarán diariamente en una hoja de ruta, que podrá estar informatizada en papel continuo, y se archivará por orden numérico en formato de libro, o en cualquier otro que respete su secuencia, conteniendo los datos que determine el Ministerio del Interior.

Los funcionarios policiales encargados de la inspección podrán requerir la exhibición de las hojas de ruta en cualquier momento, durante el desarrollo de la actividad, debiendo conservarse aquéllas, o el soporte magnético o digital en el que se consignó la información, durante cinco años, en la sede de la empresa o de las correspondientes delegaciones, o en locales de empresas especializadas en el archivo de documentación -en este caso con conocimiento del servicio policial correspondiente.

2. En el caso de transporte y distribución de explosivos, la hoja de ruta será sustituida por la documentación análoga que, para la circulación de dichas sustancias, se establece en el Reglamento de Explosivos y normativa complementaria.

Artículo 35. *Libro-registro.*

Las empresas dedicadas al transporte y distribución de títulos-valores llevarán un libro-registro, cuyo formato se ajustará a las normas que se aprueben por el Ministerio del Interior.

Artículo 36. *Comunicación previa del transporte.*

Siempre que la cuantía e importancia de los fondos, valores u objetos exceda de la cantidad o la peligrosidad de los objetos reúna las características que determine el Ministerio de Justicia e Interior, el transporte deberá ser comunicado a la dependencia correspondiente de la Dirección General de la Policía, si es urbano, y a la de la Dirección General de la Guardia Civil, si es interurbano, con veinticuatro horas de antelación al comienzo de la realización del servicio.

Artículo 37. *Otros medios de transporte.*

1. El transporte de fondos, valores y otros bienes u objetos valiosos se podrá realizar por vía aérea, utilizando los servicios ordinarios de las compañías aéreas o aparatos de vuelo propios.
2. Cuando en el aeropuerto existan caja fuerte y servicios especiales de seguridad, se podrá encargar a dichos servicios de las operaciones de carga y descarga de los bienes u objetos valiosos, con las precauciones que se señalan en los apartados siguientes.
3. Cuando en el aeropuerto no exista caja fuerte o servicios de seguridad, los vehículos blindados de las empresas de seguridad, previa facturación en la zona de seguridad de las terminales de carga, se dirigirán, con su dotación de vigilantes de seguridad y armamento reglamentario, hasta el punto desde el que se pueda realizar directamente la carga de bultos y valijas en la aeronave, debiendo permanecer en este mismo lugar hasta que se produzca el cierre y precinto de la bodega.
4. En la descarga se adoptarán similares medidas de seguridad, debiendo los vigilantes de dotación estar presentes con el vehículo blindado en el momento de la apertura de la bodega.
5. A los efectos de cumplimentar dichas obligaciones, la dirección de cada aeropuerto facilitará a las empresas de seguridad responsables del transporte las acreditaciones y permisos oportunos.
6. Análogas reglas y precauciones se seguirán para el transporte de fondos, valores y otros bienes u objetos valiosos por vía marítima.

Artículo 38. *Transporte de explosivos y objetos peligrosos.*

1. Las empresas de seguridad pueden dedicarse al transporte o a la protección del transporte de explosivos o de otras sustancias u objetos peligrosos, lo que habrá de realizarse cumpliendo lo prevenido en el presente Reglamento, en los Reglamentos de Armas y de Explosivos, y lo que se establezca al respecto en la normativa vigente, aplicable al transporte de mercancías peligrosas, debiendo ser adecuado el servicio de seguridad al riesgo a cubrir.
2. En el caso de transporte de explosivos, estos servicios se realizarán con vigilantes de seguridad, que estén en posesión de la habilitación especial prevenida al efecto en el presente Reglamento, debiendo los vehículos estar autorizados para tal finalidad por la Administración Pública competente.

Sección 6.ª Instalación y mantenimiento de aparatos, dispositivos y sistemas de seguridad

Artículo 39. *Ambito material.*

1. Únicamente las empresas autorizadas podrán realizar las operaciones de instalación y mantenimiento de aparatos, dispositivos y sistemas de seguridad electrónica contra robo e intrusión y contra incendios que se conecten a centrales receptoras de alarmas.

A efectos de su instalación y mantenimiento, tendrán la misma consideración que las centrales de alarmas los denominados centros de control o de video vigilancia, entendiendo por tales los lugares donde se centralizan los sistemas de seguridad y vigilancia de un edificio o establecimiento y que obligatoriamente deban estar controlados por personal de seguridad privada.

2. Queda prohibida la instalación de marcadores automáticos programados para transmitir alarmas directamente a las dependencias de las Fuerzas y Cuerpos de Seguridad.

Artículo 40. *Aprobación de material.*

1. Los medios materiales y técnicos, aparatos de alarma y dispositivos de seguridad que instalen y utilicen estas empresas, habrán de encontrarse debidamente aprobados con arreglo a las normas que se establezcan, impidiendo que los sistemas de seguridad instalados causen daños o molestias a terceros.

2. Los dispositivos exteriores, tales como cajas de avisadores acústicos u ópticos, deberán incorporar el teléfono de contacto desde el que se pueda adoptar la decisión adecuada, y el nombre y teléfono de la empresa que realice su mantenimiento.

Artículo 41. *Personal de las empresas.*

1. Las actividades de las empresas se realizarán por el personal que posea la titulación exigida.

2. En caso de sustitución del personal titulado, deberá comunicarse a la Dirección General de la Policía u órgano correspondiente de la Comunidad Autónoma competente, adjuntando copia compulsada del título del nuevo empleado incorporado, o el propio título, con copia, a fin de que, una vez compulsada con el original, sea devuelto éste a la empresa.

Artículo 42. *Certificado de instalación y conexión a central de alarmas.*

1. Las instalaciones de sistemas de seguridad deberán ajustarse a lo dispuesto en la normativa reguladora de las instalaciones eléctricas en lo que les sea de aplicación.

2. En los supuestos de instalación de medidas de seguridad obligatorias en empresas o entidades privadas que carezcan de Departamento de Seguridad, o cuando tales empresas o entidades se vayan a conectar a centrales de alarmas, la instalación deberá ser precedida de la elaboración y entrega al usuario de un proyecto de instalación, con niveles de cobertura adecuados a las características arquitectónicas del recinto y del riesgo a cubrir, de acuerdo con los criterios técnicos de la propia empresa instaladora y, eventualmente, los de la dependencia policial competente, todo ello con objeto de alcanzar el máximo grado posible de eficacia del sistema, de fiabilidad en la verificación de las alarmas, de colaboración del usuario, y de evitación de falsas alarmas.

3. Una vez realizada la instalación, las empresas instaladoras efectuarán las comprobaciones necesarias para asegurarse de que se cumple su finalidad preventiva y protectora, y de que es conforme con el proyecto contratado y con las disposiciones reguladoras de la materia, debiendo entregar a la entidad o establecimiento usuarios un certificado en el que conste el resultado positivo de las comprobaciones efectuadas.

4. Las instalaciones de seguridad habrán de reunir las características que se determinen por Orden del Ministro del Interior, y el certificado a que se refiere el apartado anterior deberá emitirse por ambas empresas, conjunta o separadamente, de forma que se garantice su funcionalidad global.

Artículo 43. *Revisiones.*

1. Los contratos de instalación de aparatos, dispositivos y sistemas de seguridad, en los supuestos en que la instalación sea obligatoria o cuando se conecten con una central de alarmas, comprenderán el mantenimiento de la instalación en estado operativo, con revisiones preventivas cada trimestre, no debiendo, en ningún caso, transcurrir más de cuatro meses entre dos revisiones sucesivas. En el momento de suscribir el contrato de instalación o en otro posterior, la entidad titular de la instalación podrá, sin embargo, asumir por sí misma o contratar el servicio de mantenimiento y la realización de revisiones trimestrales con otra empresa de seguridad.

2. Cuando las instalaciones permitan la comprobación del estado y del funcionamiento de cada uno de los elementos del sistema desde la central de alarmas, las revisiones preventivas tendrán una periodicidad anual, no pudiendo transcurrir más de catorce meses entre dos sucesivas.

3. Las revisiones preventivas podrán ser realizadas directamente por las entidades titulares de las instalaciones, cuando dispongan del personal con la cualificación requerida, y de los medios técnicos necesarios.

4. Las empresas de seguridad dedicadas a esta actividad y las titulares de las instalaciones llevarán libros-registros de revisiones, cuyos modelos se ajusten a las normas que se aprueben por el Ministerio de Justicia e Interior, de forma que sea posible su tratamiento y archivo mecanizado e informatizado.

Artículo 44. *Averías.*

Para el adecuado cumplimiento de lo dispuesto en el artículo anterior, las empresas de instalación y mantenimiento deberán disponer del servicio técnico adecuado que permita atender debidamente las averías de los sistemas de seguridad de cuyo mantenimiento se hayan responsabilizado, incluso en días festivos, en el plazo de veinticuatro horas siguientes al momento en que hayan sido requeridas al efecto. De las características de este servicio y de sus modificaciones, las empresas informarán oportunamente a la Dirección General de la Policía.

Artículo 45. *Manuales del sistema.*

1. Las empresas facilitarán al usuario un manual de la instalación que describirá, mediante planos y explicaciones complementarias, la distribución de las canalizaciones, el cableado, las conexiones de los equipos, las líneas eléctricas y de alarma, así como el detalle de los elementos y aparatos instalados y soportes utilizados.
2. Igualmente, entregarán un manual de uso del sistema y de su mantenimiento, que incluirá el detalle de la función que cumple cada dispositivo y la forma de usarlos separadamente o en su conjunto, así como el mantenimiento preventivo y correctivo de los aparatos o dispositivos mecánicos o electrónicos instalados, con evaluación de su vida útil, y una relación de las averías más frecuentes y de los ajustes necesarios para el buen funcionamiento del sistema.
3. En el caso de que un sistema de seguridad instalado sufra alguna variación posterior que modifique sustancialmente el originario, en todo o en parte, la empresa instaladora o, en su caso, la de mantenimiento, vendrá obligada a confeccionar nuevos manuales de instalación, uso y mantenimiento. Asimismo, la empresa instaladora deberá comunicarlo también a la central de alarmas y certificar, en la forma que se establece en el artículo 42, el resultado de las comprobaciones.

Sección 7.ª Centrales de alarmas

Artículo 46. *Requisitos de conexión.*

Para conectar aparatos, dispositivos o sistemas de seguridad a centrales de alarmas será preciso que la realización de la instalación haya sido efectuada por una empresa de seguridad inscrita en el registro correspondiente y se ajuste a lo dispuesto en los artículos 40, 42 y 43 de este Reglamento.

Artículo 47. *Información al usuario.*

Antes de efectuar la conexión, las empresas explotadoras de centrales de alarmas están obligadas a instruir al usuario del funcionamiento del servicio, informándole de las características técnicas y funcionales del sistema y de las responsabilidades que lleva consigo su incorporación al mismo.

Artículo 48. *Funcionamiento.*

1. La central de alarmas deberá estar atendida permanentemente por los operadores necesarios para la prestación de los servicios, que no podrán, en ningún caso, ser menos de dos, y que se encargarán del funcionamiento de los receptores y de la transmisión de las alarmas que reciban.
2. Cuando se produzca una alarma, las centrales deberán proceder de inmediato a su verificación con los medios técnicos y humanos de que dispongan, y comunicar seguidamente al servicio policial correspondiente las alarmas reales producidas.

Artículo 49. *Servicio de custodia de llaves.*

1. Las empresas explotadoras de centrales de alarmas podrán contratar, complementariamente, con los titulares de los recintos conectados, un servicio de custodia de llaves, de verificación de alarmas mediante desplazamiento a los propios recintos, y de respuesta a las mismas, en las condiciones que se determinen por el Ministerio del Interior, a cuyo efecto deberán disponer del armero o caja fuerte exigidos con arreglo a lo dispuesto en el artículo 25 de este Reglamento.

Las empresas industriales, comerciales o de servicios que estén autorizadas a disponer de central de alarmas, dedicada exclusivamente a su propia seguridad, podrán contratar los mismos servicios con una empresa de seguridad autorizada para vigilancia y protección.

2. Los servicios de verificación personal de las alarmas y de respuesta a las mismas se realizarán, en todo caso, por medio de vigilantes de seguridad, y consistirán, respectivamente, en la inspección del local o locales, y en el traslado de las llaves del inmueble del que procediere cada alarma, todo ello a fin de facilitar a los miembros de las Fuerzas y Cuerpos de Seguridad información sobre posible comisión de hechos delictivos y su acceso al referido inmueble.

A los efectos antes indicados, la inspección del interior de los inmuebles por parte de los vigilantes de seguridad deberá estar expresamente autorizada por los titulares de aquéllos, consignándose por escrito en el correspondiente contrato de prestación de servicios.

3. Cuando por el número de servicios de custodia de llaves o por la distancia entre los inmuebles resultare conveniente para la empresa y para los servicios policiales, aquélla podrá disponer, previa autorización de éstos, que las llaves sean custodiadas por vigilantes de seguridad sin armas en un automóvil, conectado por radio-teléfono con la central de alarmas. En este supuesto, las llaves habrán de estar codificadas, debiendo ser los códigos desconocidos por el vigilante que las porte y variados periódicamente.

4. Para los servicios a que se refieren los dos apartados anteriores, las empresas de seguridad explotadoras de centrales de alarmas podrán contar con vigilantes de seguridad, sin necesidad de estar inscritas y autorizadas para la actividad de vigilancia y protección de bienes, o bien subcontratar tal servicio con una empresa de esta especialidad.

Artículo 50. *Desconexión por falsas alarmas.*

1. En los supuestos de conexión de aparatos, dispositivos o sistemas de seguridad con una central de alarmas, con independencia de la responsabilidad y sanciones a que hubiere lugar, cuando el sistema origine dos o más falsas alarmas en el plazo de un mes, el Delegado del Gobierno, que podrá delegar en el Jefe Superior o Comisario Provincial de Policía, requerirá al titular de los bienes protegidos, a través de la dependencia policial que corresponda, para que proceda, a la mayor brevedad posible, a la subsanación de las deficiencias que dan lugar a las falsas alarmas.

2. A los efectos del presente Reglamento, se considera falsa toda alarma que no esté determinada por hechos susceptibles de producir la intervención policial. No tendrá tal consideración la mera repetición de una señal de alarma causada por una misma avería dentro de las veinticuatro horas siguientes al momento en que ésta se haya producido.

3. En caso de incumplimiento del requerimiento, se ordenará a la empresa explotadora de la central de alarma que efectúe la inmediata desconexión del sistema con la propia central, por el plazo que se estime conveniente, que podrá tener hasta un año de duración, salvo que se subsanaran en plazo más breve las deficiencias que den lugar a la desconexión, siendo la tercera desconexión de carácter definitivo, y requiriéndose para una nueva conexión el cumplimiento de lo prevenido en el artículo 42 de este Reglamento. Durante el tiempo de desconexión, el titular de la propiedad o bien protegido deberá silenciar las sirenas interiores y exteriores del sistema de seguridad.

4. Durante el tiempo que permanezca desconectado como consecuencia de ello un sistema de seguridad, su titular no podrá concertar el servicio de centralización de alarmas con ninguna empresa de seguridad.

5. Sin perjuicio de la apertura del correspondiente expediente, no se procederá a desconectar el sistema de seguridad cuando su titular estuviere obligado, con arreglo a lo dispuesto por este Reglamento, a contar con dicha medida de seguridad.

6. Cuando el titular de la propiedad o bien protegido por el sistema de seguridad no tenga contratado el servicio de centralización de alarmas y la realizare por sí mismo, se aplicará lo dispuesto en el apartado 1 de este artículo, correspondiéndole, en todo caso, la obligación de silenciar las sirenas interiores y exteriores que posea dicho sistema de seguridad, sin perjuicio de la responsabilidad en que hubiera podido incurrir.

Artículo 51. *Libros registros.*

1. Las empresas de explotación de centrales de alarma llevarán un libro-registro de alarmas, cuyo modelo se ajuste a las normas que apruebe el Ministerio del Interior, de forma que sea posible su tratamiento y archivo mecanizado e informatizado.
2. Las centrales de alarmas que tengan contratado servicio de custodia de llaves indicarán en el libro-registro de contratos cuáles de éstos incluyen aquel servicio.

TITULO II

Personal de seguridad

CAPITULO I

Habilitación y formación

Sección 1.ª Requisitos

Artículo 52. *Disposiciones comunes.*

1. El personal de seguridad privada estará integrado por: los vigilantes de seguridad, los vigilantes de explosivos, los jefes de seguridad, los directores de seguridad, los escoltas privados, los guardas particulares del campo, los guardas de caza, los guardapescas marítimos y los detectives privados.
2. A los efectos de habilitación y formación, se considerarán:

a) Los escoltas privados y los vigilantes de explosivos y sustancias peligrosas como especialidades de los vigilantes de seguridad.
b) Los guardas de caza y los guardapescas marítimos como especialidades de los guardas particulares del campo.

3. Para el desarrollo de sus respectivas funciones, el personal de seguridad privada habrá de obtener previamente la correspondiente habilitación o reconocimiento del Ministerio del Interior, con el carácter de autorización administrativa, en expediente que se instruirá a instancia de los propios interesados.
4. La habilitación o reconocimiento se documentará mediante la correspondiente tarjeta de identidad profesional, cuyas características serán determinadas por el Ministerio del Interior.
5. Los vigilantes de seguridad y los guardas particulares del campo en sus distintas modalidades habrán de disponer, además, de una cartilla profesional y de una cartilla de tiro con las características y anotaciones que se determinen por el Ministerio del Interior. La cartilla profesional y la cartilla de tiro de los vigilantes de seguridad y de los guardas particulares del campo que estén integrados en empresas de seguridad deberán permanecer depositadas en la sede de la empresa de seguridad en la que presten sus servicios.
6. De la obligación de disponer de cartilla de tiro estarán exonerados los guardapescas marítimos que habitualmente presten su servicio sin armas.
7. La habilitación o el reconocimiento para el ejercicio de la profesión de detective privado requerirá la inscripción en el registro específico regulado en el presente reglamento.

Artículo 53. *Requisitos generales.*

Para la habilitación del personal y en todo momento para la prestación de servicios de seguridad privada, el personal habrá de reunir los siguientes requisitos generales:

a) Ser mayor de edad.

b) Tener la nacionalidad de alguno de los Estados miembros de la Unión Europea o de un Estado parte en el Acuerdo sobre el Espacio Económico Europeo.

c) Poseer la aptitud física y la capacidad psíquica necesarias para el ejercicio de las respectivas funciones sin padecer enfermedad que impida el ejercicio de las mismas.

d) Carecer de antecedentes penales.

e) No haber sido condenado por intromisión ilegítima en el ámbito de protección del derecho al honor, a la intimidad personal y familiar y a la propia imagen, del secreto de las comunicaciones o de otros derechos fundamentales en los cinco años anteriores a la solicitud.

f) No haber sido sancionado en los dos o cuatro años anteriores, respectivamente, por infracción grave o muy grave en materia de seguridad.

g) No haber sido separado del servicio en las Fuerzas Armadas o en las Fuerzas y Cuerpos de Seguridad.

h) No haber ejercido funciones de control de las entidades, servicios o actuaciones de seguridad, vigilancia o investigación privadas, ni de su personal o medios, como miembro de las Fuerzas y Cuerpos de Seguridad en los dos años anteriores a la solicitud.

i) Superar las pruebas que acrediten los conocimientos y la capacitación necesarios para el ejercicio de las respectivas funciones.

Artículo 54. *Requisitos específicos.*

1. Además de los requisitos generales establecidos en el artículo anterior, el personal de seguridad privada habrá de reunir, para su habilitación, los determinados en el presente artículo, en función de su especialidad.

2. Vigilantes de seguridad y guardas particulares del campo en cualquiera de sus especialidades:

a) No haber cumplido los cincuenta y cinco años de edad.

b) Estar en posesión del título de Graduado en Educación Secundaria Obligatoria, de Técnico, u otros equivalentes a efectos profesionales, o superiores.

c) Los requisitos necesarios para poder portar y utilizar armas de fuego, a tenor de lo dispuesto al efecto en el vigente Reglamento de Armas.

3. Escoltas privados: además de los requisitos específicos de los vigilantes de seguridad, habrán de tener una estatura mínima de 1.70 metros los hombres, y de 1.65 metros las mujeres.

4. Jefes de seguridad y directores de seguridad: estar en posesión del título de Bachiller, de Técnico Superior, de Técnico en las profesiones que se determinen, u otros equivalentes a efectos profesionales, o superiores.

5. Detectives privados:

a) Estar en posesión del título de Bachiller, de Técnico Superior, de Técnico en las profesiones que se determinen, u otros equivalentes a efectos profesionales, o superiores.

b) Estar en posesión de diploma de detective privado, reconocido a estos efectos en la forma que se determine por Orden del Ministerio del Interior y obtenido después de cursar las enseñanzas programadas y de superar las correspondientes pruebas.

Artículo 55. *Fecha y acreditación.*

Los requisitos establecidos en los dos artículos anteriores deberán reunirse en la fecha de terminación del plazo de presentación de la solicitud para la participación en las pruebas a que se refiere el artículo 58 de este Reglamento ante la Secretaría de Estado de Interior, y se acreditarán en la forma que se determine en las correspondientes convocatorias.

Artículo 55 bis. *Requisitos y procedimiento para el reconocimiento.*

1. Los nacionales de Estados miembros de la Unión Europea o de Estados parte en el Acuerdo sobre el Espacio Económico Europeo, cuya habilitación o cualificación profesional haya sido obtenida en alguno de dichos Estados para el desempeño de las funciones de seguridad privada en el mismo, podrán desempeñar actividades o prestar servicios de

seguridad privada en España, siempre que, previa comprobación del Ministerio del Interior, se acredite que cumplen los siguientes requisitos:

a) Poseer alguna titulación, habilitación o certificación expedida por las autoridades competentes de cualquiera de dichos Estados, que les autorice para el ejercicio de funciones de seguridad privada en el mismo.

b) Acreditar los conocimientos, formación y aptitudes equivalentes a los exigidos en España para el ejercicio de las profesiones relacionadas con la seguridad privada. c) Tener conocimientos de lengua castellana suficientes para el normal desempeño de las funciones de seguridad privada. d) Los previstos en las letras a), d), e), f), g) y h) del artículo 53.

2. A efectos del reconocimiento que corresponde efectuar al Ministerio del Interior, se tendrá en cuenta lo previsto en la normativa sobre reconocimiento de cualificaciones profesionales.

3. La carencia o insuficiencia de conocimientos o aptitudes necesarios para el ejercicio de las actividades de seguridad privada en España de los nacionales de Estados miembros de la Unión Europea o de Estados parte en el Acuerdo sobre el Espacio Económico Europeo, podrá suplirse por aplicación de las medidas compensatorias previstas en la normativa reseñada en el párrafo anterior. 4. Una vez efectuado el citado reconocimiento, el ejercicio de las funciones de seguridad privada se regirá por lo dispuesto en este reglamento y en la normativa que lo desarrolla.

Sección 2.ª Formación

Artículo 56. *Formación previa.*

1. Los vigilantes de seguridad y los guardas particulares del campo en sus distintas modalidades habrán de superar los módulos profesionales de formación teórico-práctica asociados al dominio de las competencias que la Ley les atribuye.

Los conocimientos, habilidades, destrezas y actitudes a alcanzar en dichos módulos, así como su duración serán determinados por el Ministerio de Justicia e Interior, previo informe favorable de los Ministerios de Educación y Ciencia, y de Trabajo y Seguridad Social, así como del Ministerio de Agricultura, Pesca y Alimentación respecto a los guardas particulares del campo, y del Ministerio de Industria y Energía respecto de los vigilantes de seguridad especialidad de explosivos y sustancias peligrosas.

2. Dichos módulos formativos los impartirán los centros de formación autorizados por la Secretaría de Estado de Seguridad, los cuales habrán de disponer de un cuadro de profesores debidamente acreditados para todas las materias comprendidas en el plan de estudios, y podrán impartir, en la modalidad de formación a distancia, las enseñanzas que se determinen, exceptuando en cualquier caso las de naturaleza técnico-profesional, instrumental, de contenido técnico-operativo y las prácticas de laboratorio y de tiro, que deberán impartirse necesariamente en la modalidad "de presencia" durante el tiempo que como mínimo determine el Ministerio del Interior.

Artículo 57. *Formación permanente.*

1. Al objeto de mantener al día el nivel de aptitud y conocimientos necesarios para el ejercicio de las funciones atribuidas al personal de seguridad privada, las empresas de seguridad, a través de los centros de formación autorizados, garantizarán la organización y asistencia de su personal de seguridad privada a cursos, adaptados a las distintas modalidades de personal, de actualización en las materias que hayan experimentado modificación o evolución sustancial, o en aquellas que resulte conveniente una mayor especialización.

2. Para los vigilantes de seguridad, los cursos de actualización o especialización tendrán una duración, como mínimo, de veinte horas lectivas; cada vigilante deberá cursar al menos uno por año, y se desarrollarán en la forma que determine el Ministerio del Interior.

Sección 3.ª Procedimiento de habilitación

Artículo 58. *Pruebas. Contenido.*

Los aspirantes que hayan superado el curso o cursos a que se refiere el artículo 56 solicitarán, por sí mismos o a través de un centro de formación autorizado, su participación en las pruebas oficiales de conocimientos y capacidad que para cada especialidad establezca el Ministerio del Interior, y que versarán sobre materias sociales, jurídicas y técnicas relacionadas con las respectivas funciones, así como, en su caso, sobre destreza en el manejo de armas de fuego.

Una vez superadas las pruebas, los órganos policiales correspondientes expedirán las oportunas habilitaciones.

Artículo 59. *Documentación.*

Con la solicitud, se presentarán los documentos que acrediten el cumplimiento de los requisitos generales y específicos determinados en los artículos 53 y 54.

Artículo 60. *Organo competente.*

Las tarjetas de identidad profesional, una vez superadas las pruebas, serán expedidas por el Director general de la Policía, salvo las de los guardas particulares del campo en sus distintas modalidades, que serán expedidas por el Director general de la Guardia Civil.

Artículo 61. *Licencias de armas.*

1. Para poder prestar servicios con armas, los vigilantes de seguridad y escoltas privados, así como los guardas particulares del campo habrán de obtener licencia C en la forma prevenida en el Reglamento de Armas.

2. Dicha licencia tendrá validez exclusivamente para la prestación del servicio de seguridad, en los supuestos determinados en el presente Reglamento; carecerá de validez cuando su titular no se encuentre realizando servicios; podrá ser suspendida temporalmente por falta de realización o por resultado negativo de los ejercicios de tiro regulados en el artículo 84 de este Reglamento; y quedará sin efecto al cesar aquél en el desempeño del puesto en razón del cual le hubiera sido concedida, cualquiera que fuere la causa del cese.

Artículo 62. *Habilitación múltiple.*

Sin perjuicio de las incompatibilidades prevenidas en la Ley y en el presente Reglamento, el personal de seguridad privada podrá obtener habilitación para más de una función o especialidad y poseer en consecuencia las correspondientes tarjetas de identidad profesional.

El personal de seguridad privada que ya se encuentre diplomado o habilitado como vigilante de seguridad o como guarda particular del campo, para la obtención de diplomas o de habilitaciones complementarias, únicamente necesitará recibir la formación y/o, en su caso, superar las pruebas correspondientes a los módulos de formación profesional que sean propios del nuevo diploma o habilitación que deseen obtener, excluyéndose en consecuencia los relativos a la formación o a la habilitación que anteriormente hubieran adquirido.

Asimismo, a efectos de las habilitaciones complementarias a que se refiere el párrafo anterior, al personal que ya se encuentre habilitado como vigilante de seguridad o como guarda particular del campo, no le será aplicable el requisito de no haber cumplido cuarenta, o, en su caso, cuarenta y cinco años de edad.

Artículo 63. *Habilitación de jefes de seguridad y de directores de seguridad.*

1. Para poder ser nombrados jefes de seguridad, los solicitantes deberán haber desempeñado puestos o funciones de seguridad, pública o privada, al menos durante cinco años, y necesitarán obtener la pertinente tarjeta de identidad profesional, para lo cual habrán de acreditar, a través de las correspondientes pruebas, conocimientos suficientes sobre la normativa reguladora de la seguridad privada, la organización de servicios de seguridad y las

modalidades de prestación de los mismos, no siéndoles aplicable lo dispuesto en este reglamento sobre formación de personal.

2. La habilitación de los directores de seguridad requerirá que los solicitantes cumplan uno de los siguientes requisitos:

a) Estar en posesión de la titulación de seguridad reconocida a estos efectos por el Ministerio del Interior.

b) Acreditar el desempeño durante cinco años, como mínimo, de puestos de dirección o gestión de seguridad pública o privada, y superar las correspondientes pruebas sobre las materias que determine dicho Ministerio.

Sección 4.ª Pérdida de la habilitación

Artículo 64. *Causas.*

1. El personal de seguridad privada perderá tal condición por alguna de las siguientes causas:

a) A petición propia.

b) Por pérdida de alguno de los requisitos generales o específicos exigidos en este reglamento para el otorgamiento de la habilitación o reconocimiento.

c) Por jubilación.

d) Por ejecución de la sanción de retirada definitiva de la habilitación o reconocimiento.

2. La inactividad del personal de seguridad privada por tiempo superior a dos años exigirá la acreditación de los requisitos a que se refiere el apartado 3 del artículo 10 de la Ley de Seguridad Privada, así como la superación de las pruebas específicas que para este supuesto se determinen por el Ministerio del Interior.

Artículo 65. *Devolución de la tarjeta de identidad.*

1. En los casos a que se refiere el apartado 1 del artículo anterior, el personal de seguridad privada deberá hacer entrega, en el plazo de diez días, de su tarjeta de identidad profesional y, en su caso, de la licencia y la guía de pertenencia del arma, al jefe de seguridad o al jefe de personal de la empresa en la que presten servicios, que, a su vez, las entregará en las dependencias de la Dirección General de la Policía o de la Guardia Civil, según corresponda.

2. Los jefes de seguridad y los guardas particulares del campo no integrados en empresas de seguridad harán la referida entrega personalmente.

3. Cuando sea un detective privado con despacho propio el que pierda su condición, deberá entregar en el mismo plazo, además, salvo en el supuesto de que la actividad del despacho sea continuada por otro despacho de detective privado, el libro-registro necesario con arreglo a lo dispuesto en el artículo 108 del presente Reglamento, y depositar en la Dirección General de la Policía la documentación concerniente a las investigaciones realizadas. Dicha documentación permanecerá en el nuevo despacho de detective privado o en la Dirección General de la Policía, durante un plazo de cinco años, a disposición de las personas que hubieran encargado la investigación y tuvieran derecho a ella; y, transcurrido dicho plazo, se procederá a la destrucción de la misma.

CAPITULO II

Funciones, deberes y responsabilidades

Sección 1.ª Disposiciones comunes

Artículo 66. *Colaboración con las Fuerzas y Cuerpos de Seguridad.*

1. El personal de seguridad privada tendrá obligación especial de auxiliar a las Fuerzas y Cuerpos de Seguridad en el ejercicio de sus funciones, de prestarles su colaboración y de seguir sus instrucciones en relación con las personas, los bienes, establecimientos o

vehículos de cuya protección, vigilancia o custodia estuvieren encargados (artículo 1.4 de la L.S.P.).

2. En cumplimiento de dicha obligación y de lo dispuesto en la Ley Orgánica de Protección de la Seguridad Ciudadana, deberán comunicar a las Fuerzas y Cuerpos de Seguridad, tan pronto como sea posible, cualesquiera circunstancias o informaciones relevantes para la prevención, el mantenimiento o restablecimiento de la seguridad ciudadana, así como todo hecho delictivo de que tuviesen conocimiento en el ejercicio de sus funciones.

3. El personal de seguridad privada que sobresalga en el cumplimiento de sus funciones y especialmente en la colaboración con las Fuerzas y Cuerpos de Seguridad, podrá ser distinguido con menciones honoríficas cuyas características y procedimiento de concesión serán regulados por el Ministerio de Justicia e Interior.

Artículo 67. *Principios de actuación.*

El personal de seguridad privada se atendrá en sus actuaciones a los principios de integridad y dignidad; protección y trato correcto a las personas, evitando abusos, arbitrariedades y violencias y actuando con congruencia y proporcionalidad en la utilización de sus facultades y de los medios disponibles (artículo 1.3 de la L.S.P.).

Artículo 68. *Identificación.*

1. El personal de seguridad privada habrá de portar su tarjeta de identidad profesional y, en su caso, la licencia de armas y la correspondiente guía de pertenencia siempre que se encuentre en el ejercicio de sus funciones, debiendo mostrarlas a los miembros del Cuerpo Nacional de Policía, de la Guardia Civil, y de la Policía de la correspondiente Comunidad Autónoma o Corporación Local, cuando fueren requeridos para ello.

2. Asimismo deberá identificarse con su tarjeta de identidad profesional cuando, por razones del servicio, así lo soliciten los ciudadanos afectados, sin que se puedan utilizar a tal efecto otras tarjetas o placas.

Artículo 69. *Custodia de las armas y de sus documentaciones.*

Durante la prestación del servicio, el personal de seguridad será responsable de la custodia de sus acreditaciones, de las armas que integren su dotación, y de las documentaciones de éstas con objeto de evitar el deterioro, extravío, robo o sustracción de las mismas. Cuando tales hechos se produjeran, deberán dar conocimiento de ellos al jefe de seguridad y a las unidades orgánicas competentes de las Fuerzas y Cuerpos de Seguridad, a efectos de instrucción de los correspondientes expedientes.

Artículo 70. *Incompatibilidades.*

1. Los vigilantes, dentro de la entidad o empresa donde presten sus servicios, se dedicarán exclusivamente a la función de seguridad propia de su cargo, no pudiendo simultanear la misma con otras misiones (artículo 12.2 de la L.S.P.).

No se considerará excluida de la función de seguridad, propia de los vigilantes, la realización de actividades complementarias, directamente relacionadas con aquélla e imprescindibles para su efectividad.

2. Las funciones de escolta privado, vigilante de explosivos y detective privado son incompatibles entre sí y con las demás funciones de personal de seguridad privada aun en los supuestos de habilitación múltiple. Tampoco podrá compatibilizar sus funciones el personal de seguridad privada, salvo los jefes de seguridad, con el ejercicio de cualquier otra actividad dentro de la empresa en que realicen sus servicios.

Sección 2.ª Vigilantes de seguridad

Artículo 71. *Funciones y ejercicio de las mismas.*

1. Los vigilantes de seguridad sólo podrán desempeñar las siguientes funciones:

a) Ejercer la vigilancia y protección de bienes muebles e inmuebles, así como la protección de las personas que puedan encontrarse en los mismos.

b) Efectuar controles de identidad en el acceso o en el interior de inmuebles determinados, sin que en ningún caso puedan retener la documentación personal.

c) Evitar la comisión de actos delictivos o infracciones en relación con el objeto de su protección. d) Poner inmediatamente a disposición de los miembros de las Fuerzas y Cuerpos de Seguridad a los delincuentes en relación con el objeto de su protección, así como los instrumentos, efectos y pruebas de los delitos, no pudiendo proceder al interrogatorio de aquéllos.

e) Efectuar la protección del almacenamiento, recuento, clasificación y transporte de dinero, valores y objetos valiosos.

f) Llevar a cabo, en relación con el funcionamiento de centrales de alarma, la prestación de servicios de respuesta de las alarmas que se produzcan, cuya realización no corresponda a las Fuerzas y Cuerpos de Seguridad (artículo 11.1 de la L.S.P.).

2. Deberán seguir las instrucciones que, en el ejercicio de sus competencias impartan los responsables de las Fuerzas y Cuerpos de Seguridad, siempre que se refieran a las personas y bienes de cuya protección y vigilancia estuviesen encargados los vigilantes; colaborando con aquéllas en casos de suspensión de espectáculos, desalojo o cierre provisional de locales y, en general, dentro de los locales o establecimientos en que presten su servicio, en cualquier situación en que sea preciso para el mantenimiento y restablecimiento de la seguridad ciudadana.

3. En la organización de los servicios y en el desempeño de sus funciones, los vigilantes dependerán del jefe de seguridad de la empresa de seguridad en la que estuviesen encuadrados. No obstante, dependerán funcionalmente, en su caso, del jefe del departamento de seguridad de la empresa o entidad en que presten sus servicios.

4. En ausencia del jefe de seguridad, cuando concurran dos o más vigilantes y no estuviese previsto un orden de prelación entre ellos, asumirá la iniciativa en la prestación de los servicios el vigilante más antiguo en el establecimiento o inmueble en el que se desempeñen las funciones.

Artículo 72. *Comprobaciones previas.*

Al hacerse cargo del servicio, y si no existiese responsable de seguridad de la entidad o establecimiento, los vigilantes comprobarán el estado de funcionamiento de los sistemas de seguridad y de comunicación, si los hubiere. Deberán transmitir a los responsables de la entidad o establecimiento y a los de la empresa de seguridad las anomalías observadas, que se anotarán en el librocatálogo de medidas de seguridad. Asimismo advertirán de cualquier otra circunstancia del establecimiento o inmueble que pudiera generar inseguridad.

Artículo 73. *Diligencia.*

Los vigilantes habrán de actuar con la iniciativa y resolución que las circunstancias requieran, evitando la inhibición o pasividad en el servicio y no pudiendo negarse, sin causa que lo justifique, a prestar aquellos que se ajusten a las funciones propias del cargo, de acuerdo con las disposiciones reguladoras de la seguridad privada.

Artículo 74. *Sustituciones.*

1. Los vigilantes deberán comunicar a la empresa en la que estén encuadrados, con la máxima antelación posible, la imposibilidad de acudir al servicio y sus causas, a fin de que aquélla pueda adoptar las medidas pertinentes para su sustitución.

2. Cuando, por enfermedad u otra causa justificada, un vigilante que se encontrara prestando servicio hubiese de ser relevado por otro, lo comunicará a los responsables de seguridad del establecimiento o inmueble y a los de la empresa en que se encuentre encuadrado, con objeto de que puedan asegurar la continuidad del servicio.

Artículo 75. *Equipos caninos.*

1. Para el cumplimiento de sus funciones, los vigilantes de seguridad podrán contar con el apoyo de perros, adecuadamente amaestrados e identificados y debidamente controlados, que habrán de cumplir la regulación sanitaria correspondiente. A tal efecto, los vigilantes de seguridad deberán ser expertos en el tratamiento y utilización de los perros y portar la documentación de éstos.

2. En tales casos se habrán de constituir equipos caninos, de forma que se eviten los riesgos que los perros puedan suponer para las personas, al tiempo que se garantiza su eficacia para el servicio.

Artículo 76. *Prevenciones y actuaciones en casos de delito.*

1. En el ejercicio de su función de protección de bienes inmuebles así como de las personas que se encuentren en ellos, los vigilantes de seguridad deberán realizar las comprobaciones, registros y prevenciones necesarias para el cumplimiento de su misión.

2. No obstante, cuando observaren la comisión de delitos en relación con la seguridad de las personas o bienes objeto de protección, o cuando concurran indicios racionales de tal comisión, deberán poner inmediatamente a disposición de los miembros de las Fuerzas y Cuerpos de Seguridad a los presuntos delincuentes, así como los instrumentos, efectos y pruebas de los supuestos delitos.

Artículo 77. *Controles en el acceso a inmuebles.*

En los controles de accesos o en el interior de los inmuebles de cuya vigilancia y seguridad estuvieran encargados, los vigilantes de seguridad podrán realizar controles de identidad de las personas y, si procede, impedir su entrada, sin retener la documentación personal y, en su caso, tomarán nota del nombre, apellidos y número del documento nacional de identidad o documento equivalente de la persona identificada, objeto de la visita y lugar del inmueble a que se dirigen, dotándola, cuando así se determine en las instrucciones de seguridad propias del inmueble, de una credencial que le permita el acceso y circulación interior, debiendo retirarla al finalizar la visita.

Artículo 78. *Represión del tráfico de estupefacientes.*

Los vigilantes de seguridad deberán impedir el consumo ilegal de drogas tóxicas, estupefacientes o sustancias psicotrópicas en el interior de los locales o establecimientos o instalaciones objeto de su vigilancia y protección.

Artículo 79. *Actuación en el exterior de inmuebles.*

1. Los vigilantes sólo podrán desempeñar sus funciones en el interior de los edificios o de los inmuebles de cuya vigilancia y seguridad estuvieran encargados, salvo en los siguientes casos:

a) El transporte y distribución de monedas y billetes, títulos-valores y demás objetos que, por su valor económico y expectativas que generen o por su peligrosidad, puedan requerir protección especial.

b) La manipulación o utilización de bienes, maquinaria o equipos valiosos que hayan de tener lugar en las vías públicas o de uso común, cuando tales operaciones, bienes o equipos hayan de ser protegidos por vigilantes de seguridad, desde el espacio exterior, inmediatamente circundante.

c) Los servicios de verificación de alarmas y de respuesta a las mismas a que se refiere el artículo 49 de este Reglamento.

d) Los supuestos de persecución a delincuentes sorprendidos en flagrante delito, como consecuencia del cumplimiento de sus funciones en relación con las personas o bienes objeto de su vigilancia y protección.

e) Las situaciones en que ello viniera exigido por razones humanitarias relacionadas con dichas personas o bienes.

f) La retirada y reposición de fondos en cajeros automáticos, así como la prestación de servicios de vigilancia y protección de los cajeros durante las citadas operaciones, o en las

de reparación de averías, fuera de las horas habituales de horario al público en las respectivas oficinas.

g) Los desplazamientos excepcionales al exterior de los inmuebles objeto de protección para la realización de actividades directamente relacionadas con las funciones de vigilancia y seguridad, teniendo en cuenta, en su caso, las instrucciones de los órganos competentes de las Fuerzas y Cuerpos de Seguridad.

2. Las limitaciones previstas en el apartado precedente no serán aplicables a los servicios de vigilancia y protección de seguridad privada de los medios de transporte y de sus infraestructuras que tengan vías específicas y exclusivas de circulación, coordinados cuando proceda con los servicios de las Fuerzas y Cuerpos de Seguridad.

Artículo 80. *Servicio en polígonos industriales o urbanizaciones.*

1. El servicio de seguridad en vías de uso común pertenecientes a polígonos industriales o urbanizaciones aisladas será prestado por una sola empresa de seguridad y habrá de realizarse, durante el horario nocturno, por medio de dos vigilantes, al menos, debiendo estar conectados entre sí y con la empresa de seguridad por radiocomunicación y disponer de medios de desplazamiento adecuados a la extensión del polígono o urbanización.

2. La prestación del servicio en los polígonos industriales o urbanizaciones habrá de estar autorizada por el Gobernador civil de la provincia, previa comprobación, mediante informe de las unidades competentes de las Fuerzas y Cuerpos de Seguridad, de que concurren los siguientes requisitos:

a) Que los polígonos o urbanizaciones estén netamente delimitados y separados de los núcleos poblados.

b) Que no se produzca solución de continuidad, entre distintas partes del polígono o urbanización, por vías de comunicación ajenas a los mismos, o por otros factores. En caso de que exista o se produzca solución de continuidad, cada parte deberá ser considerada un polígono o urbanización autónomo a efectos de aplicación del presente artículo.

c) Que no se efectúe un uso público de las calles del polígono o urbanización por tráfico o circulación frecuente de vehículos ajenos a los mismos.

d) Que la administración municipal no se haya hecho cargo de la gestión de los elementos comunes y de la prestación de los servicios municipales.

e) Que el polígono o urbanización cuente con administración específica y global que permita la adopción de decisiones comunes.

3. Con independencia de lo dispuesto en el apartado 1, los titulares de los bienes que integren el polígono o urbanización podrán concertar con distintas empresas de seguridad la protección de sus respectivos locales, edificios o instalaciones, pero en este caso los vigilantes de seguridad desempeñarán sus funciones en el interior de los indicados locales, edificios o instalaciones.

4. Cuando en el cumplimiento de su misión en polígonos industriales o urbanizaciones, y con independencia del ejercicio de la función que les corresponda en el control de accesos, fuese precisa la identificación de alguna persona, los vigilantes la reflejarán en un parte de servicio, que se entregará seguidamente a las dependencias de las Fuerzas y Cuerpos de Seguridad.

Artículo 81. *Prestación de servicios con armas.*

1. Los vigilantes sólo desempeñarán con armas de fuego los siguientes servicios:

a) Los de protección del almacenamiento, recuento, clasificación, transporte y distribución de dinero, valores y objetos valiosos o peligrosos.

b) Los de vigilancia y protección de:

1.º Centros y establecimientos militares y aquellos otros dependientes del Ministerio de Defensa, en los que presten servicio miembros de las Fuerzas Armadas o estén destinados al uso por el citado personal.

2.º Fábricas, depósitos y transporte de armas, explosivos y sustancias peligrosas.

3.º Industrias o establecimientos calificados como peligrosos, con arreglo a la legislación de actividades clasificadas, por manipulación, utilización o producción de materias inflamables o explosivas que se encuentren en despoblado.

c) En los siguientes establecimientos, entidades, organismos, inmuebles y buques, cuando así se disponga por la Dirección General de la Policía y de la Guardia Civil en los supuestos no circunscritos al ámbito provincial, o por las Delegaciones o Subdelegaciones del Gobierno, valoradas circunstancias tales como la localización, el valor de los objetos a proteger, la concentración del riesgo o peligrosidad, la nocturnidad u otras de análoga significación:

1.º Dependencias de Bancos, Cajas de Ahorro y entidades de crédito.
2.º Centros de producción, transformación y distribución de energía.
3.º Centros y sedes de repetidores de comunicación.
4.º Polígonos industriales y lugares donde se concentre almacenamiento de materias primas o mercancías.
5.º Urbanizaciones aisladas.
6.º Joyerías, platerías o lugares donde se fabriquen, almacenen o exhiban objetos preciosos.
7.º Museos, salas de exposiciones o similares.
8.º Los lugares de caja o donde se concentren fondos, de grandes superficies comerciales o de casinos de juego.
9.º Buques mercantes y buques pesqueros que naveguen bajo bandera española en aguas en las que exista grave riesgo para la seguridad de las personas o de los bienes, o para ambos.

2. Cuando las empresas, organismos o entidades titulares de los establecimientos o inmuebles entendiesen que en supuestos no incluidos en el apartado anterior el servicio debiera ser prestado con armas de fuego, teniendo en cuenta las circunstancias que en el mismo se mencionan, solicitarán la correspondiente autorización a la Dirección General de la Policía y de la Guardia Civil, respecto a supuestos no circunscritos al ámbito provincial o a las Delegaciones o Subdelegaciones del Gobierno, que resolverán lo procedente, pudiendo autorizar la formalización del correspondiente contrato.

Artículo 82. *Depósito de las armas.*

1. Los vigilantes no podrán portar las armas fuera de las horas y de los lugares de prestación del servicio, debiendo el tiempo restante estar depositadas en los armeros de los lugares de trabajo o, si no existieran, en los de la empresa de seguridad.
2. Excepcionalmente, a la iniciación y terminación del contrato de servicio o, cuando se trate de realizar servicios especiales, suplencias, o los ejercicios obligatorios de tiro, podrán portar las armas en los desplazamientos anteriores y posteriores, previa autorización del jefe de seguridad o, en su defecto, del responsable de la empresa de seguridad, que habrá de ajustarse a las formalidades que determine el Ministerio de Justicia e Interior, debiendo entregarlas para su depósito en el correspondiente armero.
A los efectos previstos en el párrafo anterior, se considerarán servicios especiales aquéllos cuya duración no exceda de un mes.

Artículo 83. *Responsabilidad por la custodia de las armas.*

1. Las empresas de seguridad serán responsables de la conservación, mantenimiento y buen funcionamiento de las armas, y los vigilantes, de la seguridad, cuidado y uso correcto de las que tuvieran asignadas, durante la prestación del servicio.
2. De la obligación de depositar el arma en el armero del lugar de trabajo serán responsables el vigilante y el jefe de seguridad, y de la relativa a depósito en el armero de la empresa de seguridad, el vigilante y el jefe de seguridad o director de la empresa de seguridad.
3. Del extravío, robo o sustracción de las armas, así como, en todo caso, de su ausencia del armero cuando deban estar depositadas en el mismo se deberá dar cuenta inmediata a las dependencias de las Fuerzas y Cuerpos de Seguridad.

Artículo 84. *Ejercicios de tiro.*

1. Los vigilantes de seguridad que presten servicios con armas deberán realizar un ejercicio de tiro obligatorio al semestre, y los demás que puedan prestar dichos servicios, por estar en posesión de las correspondientes licencias de armas, aunque las mismas se encuentren depositadas en las Intervenciones de Armas de la Guardia Civil, un ejercicio de tiro obligatorio al año. En ambos casos, se efectuará el número de disparos que se determine por el Ministerio del Interior. No deberán transcurrir más de ocho meses entre dos ejercicios sucesivos de los primeros, ni más de catorce meses entre dos ejercicios sucesivos de los segundos.

La falta de realización o el resultado negativo de un ejercicio de tiro podrá dar lugar a la suspensión temporal de la correspondiente licencia de armas hasta que el ejercicio se realice con resultado positivo.

2. Si fuere necesario, para los ejercicios obligatorios de tiro de los vigilantes que no tuviesen asignadas armas, se trasladarán por el jefe o responsable de seguridad de la empresa las que ésta posea con tal objeto, efectuándose el traslado con la protección de un vigilante armado, yendo las armas descargadas y separadas de la cartuchería, de acuerdo con lo dispuesto en el Reglamento de Armas.

Artículo 85. *Pruebas psicotécnicas periódicas.*

Los vigilantes que presten o puedan prestar servicio con armas deberán superar, con una periodicidad de cinco años, las pruebas psicotécnicas que determine el Ministerio de Justicia e Interior, periodicidad que será bienal a partir de los cincuenta y cinco años de edad, cuyo resultado se comunicará a la Intervención de Armas. En caso de no realización o superación de las pruebas, los interesados no podrán desempeñar servicios con armas, debiendo hacer entrega de la correspondiente licencia, para su anulación, a la Intervención de Armas.

Artículo 86. *Arma de fuego y medios de defensa.*

1. El arma reglamentaria de los vigilantes de seguridad en los servicios que hayan de prestarse con armas será la que determine el Ministerio del Interior.

2. Los vigilantes de seguridad portarán la defensa que se determine por el Ministerio del Interior, en los supuestos que asimismo se determinen por dicho Ministerio.

3. Cuando los vigilantes en el ejercicio de sus funciones hayan de proceder a la detención e inmovilización de personas para su puesta a disposición de las Fuerzas y Cuerpos de Seguridad, el jefe de seguridad podrá disponer el uso de grilletes.

4. En los supuestos previstos en el nº 9 de la letra c) del apartado 1 del artículo 81 anterior, los vigilantes de seguridad privada podrán portar y usar armas de guerra para la prestación de servicios de protección de personas y bienes, previniendo y repeliendo ataques, con las características, en las condiciones y con los requisitos que se determinen, de manera conjunta, por los Ministerios de Defensa y de Interior.

Artículo 87. *Uniforme y distintivos.*

1. Las funciones de los vigilantes de seguridad únicamente podrán ser desarrolladas vistiendo el uniforme y ostentando el distintivo del cargo que sean preceptivos, que serán aprobados por el Ministerio de Justicia e Interior, teniendo en cuenta las características de las funciones respectivas de las distintas especialidades de vigilantes y que no podrán confundirse con los de las Fuerzas Armadas ni con los de las Fuerzas y Cuerpos de Seguridad (artículo 12.1 de la L.S.P.).

2. Los vigilantes no podrán vestir el uniforme ni hacer uso de sus distintivos fuera de las horas y lugares del servicio y de los ejercicios de tiro.

Sección 3.ª Escoltas privados

Artículo 88. *Funciones.*

1. Son funciones de los escoltas privados, con carácter exclusivo y excluyente, el acompañamiento, defensa y protección de personas determinadas, que no tengan la condición de autoridades públicas, impidiendo que sean objeto de agresiones o actos delictivos (artículo 17.1 de la L.S.P.).
2. La defensa y protección a prestar ha de estar referida únicamente a la vida e integridad física y a la libertad de las personas objeto de protección.

Artículo 89. *Forma de prestación del servicio.*

En el desempeño de sus funciones, los escoltas no podrán realizar identificaciones o detenciones, ni impedir o restringir la libre circulación, salvo que resultase imprescindible como consecuencia de una agresión o de un intento manifiesto de agresión a la persona protegida o a los propios escoltas, debiendo en tal caso poner inmediatamente al detenido o detenidos a disposición de las Fuerzas y Cuerpos de Seguridad, sin proceder a ninguna suerte de interrogatorio.

Artículo 90. *Uso de armas y ejercicios de tiro.*

1. El arma reglamentaria de los escoltas privados será la que determine el Ministerio de Justicia e Interior.
2. Portarán las armas con discreción y sin hacer ostentación de ellas, pudiendo usarlas solamente en caso de agresión a la vida, integridad física o libertad, y atendiendo a criterios de proporcionalidad con el medio utilizado para el ataque.
3. Los escoltas privados podrán portar sus armas solamente cuando se encuentren en el ejercicio de sus funciones, debiendo depositarlas, a la finalización de cada servicio, en el armero de la empresa a la que pertenezcan, o en el del lugar de trabajo o residencia de la persona protegida.
4. Cuando por razones de trabajo se hallasen, al finalizar el servicio, en localidad distinta de aquélla en la que radique la sede de su empresa, el arma se depositará en el armero de la delegación de la empresa, si la hubiese. En caso contrario, el arma quedará bajo la custodia del escolta, con la autorización, con arreglo al artículo 82, del jefe de seguridad de la empresa.
5. Los escoltas privados deberán realizar ejercicios obligatorios de tiro, una vez cada trimestre, y les será de aplicación lo dispuesto en este Reglamento para los vigilantes de seguridad, sobre número de disparos, conservación y mantenimiento de las armas que tuvieren asignadas, así como lo establecido respecto a la autorización para su traslado con ocasión de los ejercicios obligatorios de tiro.

Artículo 91. *Régimen general.*

A los escoltas privados les será de aplicación lo establecido para los vigilantes de seguridad sobre:

a) Colaboración con las Fuerzas y Cuerpos de Seguridad.
b) Diligencia en la prestación del servicio.
c) Sustituciones.
d) Conservación de las armas.
e) Pruebas psicotécnicas periódicas.

Sección 4.ª Guardas particulares del campo

Artículo 92. *Funciones.*

Los guardas particulares del campo, en sus distintas modalidades, ejercerán las funciones de vigilancia y protección de la propiedad:

a) En las fincas rústicas.

b) En las fincas de caza, en cuanto a los distintos aspectos del régimen cinegético.
c) En los establecimientos de acuicultura y zonas marítimas protegidas con fines pesqueros.

Artículo 93. *Arma reglamentaria.*

1. El arma reglamentaria de los guardas particulares del campo será el arma de fuego larga para vigilancia y guardería, determinada con arreglo a lo dispuesto en el artículo 3 del Reglamento de Armas.
2. Cuando el guarda esté encuadrado en una empresa de seguridad, al finalizar el servicio depositará el arma en el armero de aquélla, si tuviese su sede o delegación en la localidad de prestación del servicio; y, en caso contrario, el arma quedará bajo la custodia del guarda.
3. Solamente se podrán prestar con armas los servicios de vigilancia de terrenos cinegéticos y aquellos otros que autorice el Gobernador Civil, teniendo en cuenta los supuestos y circunstancias enumerados en el artículo 81 de este Reglamento.

Artículo 94. *Régimen general.*

A los guardas particulares del campo les será de aplicación lo establecido para los vigilantes de seguridad sobre:

a) Colaboración con las Fuerzas y Cuerpos de Seguridad.
b) Disposición de cartilla de tiro.
c) Diligencia en la prestación del servicio.
d) Sustituciones.
e) Utilización de perros.
f) Controles y actuaciones en casos de delito.
g) Ejercicios de tiro, cuya periodicidad será anual.
h) Conservación de armas.
i) Pruebas psicotécnicas periódicas.
j) Utilización de uniformes y distintivos.
k) Comprobaciones previas a la iniciación de los servicios.

Sección 5.ª Jefes y directores de seguridad

Artículo 95. *Funciones.*

1. A los jefes de seguridad les corresponde, bajo la dirección de las empresas de que dependan, el ejercicio de las siguientes funciones:

a) El análisis de situaciones de riesgo y la planificación y programación de las actuaciones precisas para la implantación y realización de los servicios de seguridad.
b) La organización, dirección e inspección del personal y servicios de seguridad privada.
c) La propuesta de los sistemas de seguridad que resulten pertinentes, así como la supervisión de su utilización, funcionamiento y conservación.
d) El control de la formación permanente del personal de seguridad que de ellos dependa, proponiendo a la dirección de la empresa la adopción de las medidas o iniciativas adecuadas para el cumplimiento de dicha finalidad.
e) La coordinación de los distintos servicios de seguridad que de ellos dependan, con actuaciones propias de protección civil, en situaciones de emergencia, catástrofe o calamidad pública.
f) Asegurar la colaboración de los servicios de seguridad con los de las correspondientes dependencias de las Fuerzas y Cuerpos de Seguridad.
g) En general, velar por la observancia de la regulación de seguridad aplicable.
h) La dirección de los ejercicios de tiro del personal de seguridad a sus órdenes, si poseyeran la cualificación necesaria como instructores de tiro.

2. A los directores de seguridad les corresponde el ejercicio de las funciones enumeradas en los apartados a), b), c), e), f) y g) del artículo anterior.

Artículo 96. *Supuestos de existencia obligatoria.*

1. Los servicios de seguridad se prestarán obligatoriamente bajo la dirección de un jefe de seguridad, en las empresas de seguridad inscritas para todas o alguna de las actividades previstas en el artículo 1.1, párrafos a), b), c) y d), del presente reglamento, y en las delegaciones o sucursales abiertas de acuerdo con lo dispuesto en el artículo 17, apartados 2 y 3 de este reglamento.

2. El mando de los servicios de seguridad se ejercerá por un director de seguridad designado por la entidad, empresa o grupo empresarial:

a) En las empresas o entidades que constituyan, en virtud de disposición general o decisión gubernativa, departamento de seguridad.

b) En los centros, establecimientos o inmuebles que cuenten con un servicio de seguridad integrado por veinticuatro o más vigilantes de seguridad o guardas particulares del campo, y cuya duración prevista supere un año. c) Cuando así lo disponga la Dirección General de la Policía y de la Guardia Civil para los supuestos supraprovinciales, o el Subdelegado del Gobierno de la provincia, atendiendo el volumen de medios personales y materiales, tanto físicos como electrónicos, el sistema de seguridad de la entidad o establecimiento, así como la complejidad de su funcionamiento y el grado de concentración de riesgo.

Artículo 97. *Comunicación con las Fuerzas y Cuerpos de Seguridad.*

Los jefes de seguridad, así como los directores de seguridad, canalizarán hacia las dependencias de las Fuerzas y Cuerpos de Seguridad las comunicaciones a que se refiere el artículo 66 de este Reglamento, y deberán comparecer a las reuniones informativas o de coordinación a que fueren citados por las autoridades policiales competentes.

Artículo 98. *Subsanación de deficiencias o anomalías.*

Los jefes y los directores de seguridad deberán proponer o adoptar las medidas oportunas para la subsanación de las deficiencias o anomalías que observen o les comuniquen los vigilantes o los guardas particulares del campo en relación con los servicios o los sistemas de seguridad, asegurándose de la anotación, en este último caso, de la fecha y hora de la subsanación en el correspondiente libro-catálogo y comprobando su funcionamiento.

Artículo 99. *Delegación de funciones.*

Los jefes de seguridad podrán delegar únicamente el ejercicio de las facultades para autorizar el traslado de armas o la obligación de efectuar personalmente el traslado, y las relativas a comunicación con las Fuerzas y Cuerpos de Seguridad y a subsanación de deficiencias o anomalías, así como las de dirección e inspección del personal y servicios de seguridad privada, lo que requerirá la aprobación de las empresas, y habrá de recaer, donde no hubiera jefe de seguridad delegado, en persona del Servicio o Departamento de Seguridad que reúna análogas condiciones de experiencia y capacidad que ellos; comunicando a las dependencias de las Fuerzas y Cuerpos de Seguridad el alcance de la delegación y la persona o personas de la empresa en quienes recae, con expresión del puesto que ocupa en la propia empresa. Asimismo deberán comunicar a dichas dependencias cualquier variación que se produzca al respecto, y en su caso la revocación de la delegación.

Artículo 100. *Comunicación de altas y bajas.*

Las empresas de seguridad y las entidades con departamento de seguridad comunicarán a la Dirección General de la Policía las altas y bajas de los jefes de seguridad y de los directores de seguridad, respectivamente, dentro de los cinco días siguientes a la fecha en que se produzcan.

Sección 6.ª Detectives privados

Artículo 101. *Funciones.*

1. Los detectives privados, a solicitud de personas físicas o jurídicas, se encargarán:

a) De obtener y aportar información y pruebas sobre conductas o hechos privados.
b) De la investigación de delitos perseguibles sólo a instancia de parte por encargo de los legitimados en el proceso penal.
c) De la vigilancia en ferias, hoteles, exposiciones o ámbitos análogos (artículo 19.1 de la L.S.P.).

2. A los efectos del presente artículo, se considerarán conductas o hechos privados los que afecten al ámbito económico, laboral, mercantil, financiero y, en general, a la vida personal, familiar o social, exceptuada la que se desarrolle en los domicilios o lugares reservados.
3. En el ámbito del apartado 1.c) se consideran comprendidas las grandes superficies comerciales y los locales públicos de gran concurrencia.

Artículo 102. *Prohibiciones.*

1. Los detectives no podrán realizar investigaciones sobre delitos perseguibles de oficio, debiendo denunciar inmediatamente ante la autoridad competente cualquier hecho de esta naturaleza que llegara a su conocimiento y poniendo a su disposición toda la información y los instrumentos que pudieran haber obtenido, relacionados con dichos delitos.
2. En ningún caso podrán utilizar para sus investigaciones medios personales o técnicos que atenten contra el derecho al honor, a la intimidad personal o familiar, a la propia imagen o al secreto de las comunicaciones (artículo 19.3 y 4 de la Ley de S.P.).

Artículo 103. *Carácter reservado de las investigaciones.*

Los detectives privados están obligados a guardar riguroso secreto de las investigaciones que realicen y no podrán facilitar datos sobre éstas más que a las personas que se las encomienden y a los órganos judiciales y policiales competentes para el ejercicio de sus funciones.

Artículo 104. *Registro especial.*

1. Por la Dirección General de la Policía se llevará un Registro de detectives privados con despacho abierto, en el que, con el número de orden de inscripción, figurará su nombre y apellidos, domicilio social y, en su caso, detectives asociados o dependientes, habilitados de acuerdo con lo dispuesto en los preceptos aplicables de los artículos 52 a 65 de este Reglamento, y delegaciones o sucursales que de aquéllos dependan, así como el nombre comercial que utilicen. La Dirección General de la Policía comunicará oportunamente estos datos al órgano correspondiente de la Comunidad Autónoma competente.
2. Para el comienzo del desarrollo de las funciones del detective privado y de sus detectives asociados, la apertura del despacho deberá estar reseñada en el Registro a que se refiere el apartado anterior, y hallarse en posesión el titular y los asociados de las correspondientes tarjetas de identidad profesional. No se podrá hacer publicidad de las actividades propias de los detectives privados sin estar inscrito en el Registro.
3. La inscripción del despacho en dicho Registro se practicará previa instrucción de procedimiento, iniciado a solicitud de persona interesada, en el que habrá de acreditarse, si ya no lo estuviere en el órgano encargado del Registro, el cumplimiento de los requisitos generales que se determinan en el artículo 53 de este Reglamento, y de los específicos señalados en el artículo 54.5 del mismo, así como el de haber causado alta en el Impuesto de Actividades Económicas.
4. La inscripción de detectives dependientes o asociados se acordará previa solicitud del detective titular del despacho de que dependan, adjuntando, en caso de vinculación laboral, documento acreditativo del alta de aquéllos en la Seguridad Social.

5. A los procedimientos de inscripción de despachos de detectives privados les será de aplicación lo dispuesto en los artículos 8 y 9 de este Reglamento, sobre subsanación de defectos, resoluciones, notificaciones y recursos.

6. El número de orden de inscripción y la fecha en que se hubiere acordado se comunicará al interesado, que deberá hacer constar dicho número en su publicidad, documentos e informes.

7. Cualquier variación de los datos registrales, así como de los relativos a detectives dependientes o asociados y a delegaciones o sucursales, se comunicará, en el plazo de los quince días siguientes a la fecha en que se produzca, a efectos de su posible incorporación al Registro especial, a la Dirección General de la Policía, que la transmitirá oportunamente al órgano correspondiente de la Comunidad Autónoma competente.

Artículo 105. *Sociedades de detectives.*

1. Las sociedades mercantiles, laborales o cooperativas de detectives habrán de estar constituidas únicamente por personas físicas reglamentariamente habilitadas como tales, debiendo remitir a la Dirección General de la Policía, a efectos de inscripción en el Registro, copia autorizada de la escritura de constitución de la sociedad y certificado o nota de inscripción de la misma en el Registro correspondiente, así como de cualquier modificación que se produzca en la composición de los órganos de administración de la sociedad o en la titularidad de las acciones o participaciones representativas de su capital y en los aumentos o disminuciones de éste. La comunicación deberá remitirse a la Dirección General de la Policía en los quince días siguientes a la fecha en que se otorgue la correspondiente escritura o se produzca la modificación en cuestión, correspondiendo al citado centro directivo dar traslado de la comunicación a la Comunidad Autónoma competente.

2. Los miembros de estas sociedades únicamente podrán dedicarse a la realización de las actividades propias de los detectives, no pudiendo desarrollar ninguna de las atribuidas con carácter exclusivo a las empresas de seguridad.

Artículo 106. *Establecimiento de sucursales.*

Los detectives privados podrán establecer departamentos delegados o sucursales en la misma localidad donde tengan establecido su despacho profesional o en otras distintas, debiendo, en todo caso, estar dirigido cada uno de ellos por un detective habilitado o reconocido con arreglo a lo dispuesto en este reglamento, distinto del titular de la oficina principal.

Artículo 107. *Apertura de sucursales.*

Para la efectividad de lo dispuesto en el artículo anterior, deberán comunicar previamente a la Dirección General de la Policía, que dará traslado a la Comunidad Autónoma competente, la apertura de la delegación o sucursal, con la determinación de su localización, y acompañando los documentos relativos a los detectives que vayan a trabajar en la misma.

Artículo 108. *Libro-registro.*

1. En cada despacho y sucursal, los detectives llevarán un libro-registro, según el modelo que se apruebe por el Ministerio del Interior, concebido de forma que su tratamiento y archivo pueda ser mecanizado e informatizado.

2. La obligación de llevanza del libro-registro del apartado anterior también corresponderá a los nacionales de Estados miembros de la Unión Europea o de Estados parte en el Acuerdo sobre el Espacio Económico Europeo habilitados como detectives privados en cualquiera de dichos Estados y que pretendan ejercer su profesión en España sin disponer de despacho o sucursal en nuestro país.

Artículo 109. *Comunicación de informaciones.*

Los detectives titulares y los asociados o dependientes, cuando sean requeridos para ello por los órganos competentes de la Administración de Justicia, y de las Fuerzas y

Cuerpos de Seguridad, deberán facilitar las informaciones de que tuvieran conocimiento en relación con las investigaciones que tales organismos se encontraran llevando a cabo.

Artículo 110. *Responsabilidad.*

Los detectives privados y las sociedades de detectives responderán civilmente de las acciones u omisiones en que, durante la ejecución de sus servicios, incurran los detectives dependientes o asociados que con ellos estén vinculados.

TITULO III

Medidas de seguridad

CAPITULO I

Medidas de seguridad en general

Sección 1.ª Disposiciones comunes

Artículo 111. *Obligatoriedad.*

1. De acuerdo con lo dispuesto en el artículo 13 y en la disposición adicional de la Ley Orgánica 1/1992, sobre protección de la seguridad ciudadana, y con la finalidad de prevenir la comisión de actos delictivos, la Secretaría de Estado de Interior, para supuestos supraprovinciales, o los Gobernadores Civiles podrán ordenar que las empresas industriales, comerciales o de servicios adopten las medidas de seguridad que, con carácter general o para supuestos específicos, se establecen en el presente Reglamento.

2. Las obras que resulte preciso efectuar en los establecimientos, para la adopción de las medidas de seguridad obligatorias, serán comunicadas al arrendador, si bien éste no podrá oponerse a ellas, salvo que provoquen una disminución de la estabilidad o seguridad del edificio. Al concluir el contrato, el arrendador podrá optar entre exigir al arrendatario que reponga las cosas al estado anterior, o conservar la modificación efectuada, sin que éste pueda reclamar indemnización alguna.

Sección 2.ª Servicios y sistemas de seguridad

Artículo 112. *Enumeración de los servicios o sistemas y circunstancias determinantes.*

1. Cuando la naturaleza o importancia de la actividad económica que desarrollan las empresas y entidades privadas, la localización de sus instalaciones, la concentración de sus clientes, el volumen de los fondos o valores que manejen, el valor de los bienes muebles u objetos valiosos que posean, o cualquier otra causa lo hiciesen necesario, el Secretario de Estado de Interior para supuestos supraprovinciales, o los Gobernadores Civiles, podrán exigir a la empresa o entidad que adopte, conjunta o separadamente, los servicios o sistemas de seguridad siguientes:

a) Creación del departamento de seguridad.

b) Establecimiento del servicio de vigilantes de seguridad, con o sin armas a cargo de personal integrado en empresas de seguridad.

c) Instalación de dispositivos y sistemas de seguridad y protección.

d) Conexión de los sistemas de seguridad con centrales de alarmas, ajenas o propias, que deberán ajustarse en su funcionamiento a los establecido en los artículos 46, 48 y 49, y reunir los requisitos que se establecen en el apartado 6.2 del anexo del presente Reglamento; no pudiendo prestar servicios a terceros si las empresas o entidades no están habilitadas como empresas de seguridad.

2. En todo caso deberá existir Departamento de Seguridad cuando concurran las circunstancias de los párrafos b) y c) del artículo 96.2 de este Reglamento.

Artículo 113. *Implantación en organismos públicos.*

Si se considerase necesaria la implantación de dichos servicios o sistemas de seguridad en empresas, entidades u organismos públicos, el Director general de la Policía para supuestos supraprovinciales, o los Gobernadores Civiles elevarán al Ministro de Justicia e Interior la correspondiente propuesta para que, previo acuerdo con el Ministerio o Administración de los que dependan las instalaciones o locales necesitados de protección, dicte la resolución procedente.

En forma análoga se procederá por los órganos correspondientes de las Comunidades Autónomas competentes, cuando se trate de empresas, entidades u organismos públicos dependientes de la Administración Autonómica o de la Administración Local.

Artículo 114. *Servicio sustitutorio de vigilantes de seguridad.*

Cuando por dificultades técnicas o carencia de equipos adecuados fuera imposible la conexión del sistema de seguridad con una central privada de alarmas, las empresas y entidades a que se refiere el artículo 112, que debieran establecer tal sistema de seguridad, podrán ser obligadas, por el tiempo en que persista la imposibilidad técnica, a la implantación del servicio de vigilantes de seguridad, con personal perteneciente a empresas de seguridad.

Artículo 115. *Departamento de seguridad facultativo.*

Las empresas industriales, comerciales o de servicios, y las entidades públicas y privadas, que, sin estar obligadas a ello -por no estar comprendidas en los supuestos regulados en el artículo 96 del presente Reglamento-, pretendan organizar su departamento de seguridad, con todos o alguno de los cometidos enumerados en el artículo siguiente, deberán disponer de un director de seguridad al frente del mismo, y comunicarlo a la Subdelegación del Gobierno, si el ámbito de actuación no excediera del territorio de una provincia, y, en todo caso, al Director general de la Policía.

Artículo 116. *Cometidos del departamento de seguridad.*

El departamento de seguridad obligatoriamente establecido, único para cada entidad, empresa o grupo empresarial y con competencia en todo el ámbito geográfico en que éstos actúen, comprenderá la administración y organización de los servicios de seguridad de la empresa o grupo, incluso, en su caso, del transporte y custodia de efectos y valores, correspondiéndole la dirección de los vigilantes de seguridad o guardas particulares del campo, el control del funcionamiento de las instalaciones de sistemas físicos y electrónicos, así como del mantenimiento de éstos y la gestión de las informaciones que generen.

Artículo 117. *Organización del departamento de seguridad.*

En aquellas entidades y empresas de seguridad en las que el departamento de seguridad se caracterice por su gran volumen y complejidad, en dicho departamento existirá, bajo la dirección de seguridad, a la que corresponderán las funciones del director de seguridad, la estructura necesaria con los escalones jerárquicos y territoriales adecuados, al frente de los cuales se encontrarán los delegados correspondientes.

Artículo 118. *Dispensa del servicio de vigilantes de seguridad.*

1. En los casos en que, en uso de las facultades que confiere este Reglamento, se requiera la implantación del servicio de vigilantes de seguridad, el Director general de la Policía en supuestos supraprovinciales, o los Gobernadores Civiles, a petición de la empresa o entidad interesada, dispensarán de la implantación o mantenimiento del servicio de vigilantes de seguridad o de guardas particulares del campo en los centros o establecimientos, cuando aquélla acredite la instalación y el adecuado funcionamiento de las medidas de seguridad específicamente reguladas en el presente Reglamento.

2. La solicitud de dispensa se presentará ante dichas autoridades, que comprobarán la instalación y el adecuado funcionamiento de tales medidas de seguridad a través de la inspección que realicen los funcionarios competentes del Cuerpo Nacional de Policía, o, en

su caso, del Cuerpo de la Guardia Civil, y resolverán lo procedente, recabando previamente el parecer de los representantes de los trabajadores, que habrán de expresarlo dentro de un plazo de diez días.

CAPITULO II

Medidas de seguridad específicas

Sección 1.ª Bancos, cajas de ahorro y demás entidades de credito

Artículo 119. *Departamento de seguridad y central de alarmas.*

1. En todos los bancos, cajas de ahorro y demás entidades de crédito, existirá un departamento de seguridad, que tendrá a su cargo la organización y administración de la seguridad de la entidad bancaria o de crédito, de acuerdo con lo dispuesto en el artículo 116 de este Reglamento.

2. Asimismo, dichas entidades deberán conectar con una central de alarmas propia o ajena los sistemas de seguridad instalados en sus establecimientos y oficinas, salvo que dificultades técnicas hicieran imposible la conexión, en cuyo caso les será de aplicación lo dispuesto en el artículo 114.

3. Las centrales de alarmas propias de una entidad de crédito, que habrán de ajustarse en su funcionamiento a lo establecido en los artículos 46, 48 y 49, y reunir los requisitos del apartado 6.2 del anexo de este Reglamento, podrán prestar servicios a los distintos establecimientos de la misma entidad o de sus filiales.

Artículo 120. *Medidas de seguridad concretas.*

1. En los establecimientos u oficinas de las entidades de crédito donde se custodien fondos o valores, deberán ser instalados, en la medida que resulte necesaria en cada caso teniendo en cuenta las circunstancias enumeradas en el artículo 112 de este Reglamento y los criterios que se fijen por el Ministerio de Justicia e Interior, oyendo a la Comisión Mixta Central de Seguridad Privada:

a) Equipos o sistemas de captación y registro, con capacidad para obtener las imágenes de los autores de delitos contra las personas y contra la propiedad, cometidos en los establecimientos y oficinas, que permitan la posterior identificación de aquéllos, y que habrán de funcionar durante el horario de atención al público, sin que requieran la intervención inmediata de los empleados de la entidad.

Los soportes destinados a la grabación de imágenes han de estar protegidos contra robo, y la entidad de ahorro o de crédito deberá conservar los soportes con las imágenes grabadas durante quince días al menos desde la fecha de la grabación, en que estarán exclusivamente a disposición de las autoridades judiciales y de las dependencias de las Fuerzas y Cuerpos de Seguridad, a las que facilitarán inmediatamente aquellas que se refieran a la comisión de hechos delictivos.

El contenido de los soportes será estrictamente reservado, y las imágenes grabadas únicamente podrán ser utilizadas como medio de identificación de los autores de delitos contra las personas y contra la propiedad, debiendo ser inutilizados el contenido de los soportes y las imágenes una vez transcurridos quince días desde la grabación, salvo que hubiesen dispuesto lo contrario las autoridades judiciales o las Fuerzas y Cuerpos de Seguridad competentes.

b) Dispositivos electrónicos, de las características que se determinen por el Ministerio de Justicia e Interior, con capacidad para detectar el ataque a cualquier elemento de seguridad física donde se custodien efectivo o valores.

c) Pulsadores u otros medios de accionamiento fácil de las señales de alarma.

d) Recinto de caja de, al menos, dos metros de altura y que deberá estar cerrado desde su interior durante las horas de atención al público, siempre que el personal se encuentre dentro del mismo, protegido con blindaje antibala del nivel que se determine y dispositivo capaz de impedir el ataque a las personas situadas en su interior.

e) Control individualizado de accesos a la oficina o establecimiento, que permita la detección de masas metálicas, bloqueo y anclaje automático de puertas, y disponga de mando a distancia para el desbloqueo del sistema en caso de incendio o catástrofe, o puerta de emergencia complementaria, detectores de presencia o zócalos sensibles en vía de salida cuando se utilice el sistema de doble vía, y blindaje que se determine.

f) Carteles del tamaño que se determine por el Ministerio de Justicia e Interior u otros sistemas de información de análoga eficacia, anunciadores de la existencia de medidas de seguridad, con referencia expresa al sistema de apertura automática retardada y, en su caso, al sistema permanente de captación de imágenes.

2. Los establecimientos y oficinas de crédito situadas en localidades con población inferior a diez mil habitantes, y que además no cuenten con más de diez empleados, estarán exceptuadas de la obligación de implantar las medidas de seguridad enumeradas bajo los párrafos d) y e) del apartado anterior.

En las restantes oficinas o establecimientos, las entidades deberán instalar, en su caso, una de las dos medidas de seguridad incluidas bajo los párrafos d) y e) del apartado 1, pudiendo optar voluntariamente por cualquiera de ellas. No obstante, la Dirección General de la Policía en supuestos que excedan del territorio de una provincia, o el Gobierno Civil, a petición de la entidad interesada, oyendo a la representación de los trabajadores que habrá de expresar su parecer dentro de un plazo de diez días, y previa valoración de las circunstancias a que se refiere el artículo 112.1 de este Reglamento, podrá autorizar la sustitución de cualquiera de dichas medidas por la implantación del servicio de vigilantes de seguridad.

3. En la determinación de las medidas de seguridad a implantar en las oficinas de las entidades de crédito sitas en las Delegaciones y Administraciones de la Agencia Estatal de Administración Tributaria, y que presten servicio de caja en las mismas, la autoridad gubernativa competente deberá oír previamente a la Delegación o Administración afectada.

Artículo 121. *Requisitos de las cámaras acorazadas y de cajas de alquiler.*

Las cámaras acorazadas de efectivo y de compartimentos de alquiler deberán tener las características y el nivel de resistencia que determine el Ministerio del Interior, y estar provistas de las siguientes medidas de seguridad:

a) Dispositivo mecánico o electrónico que permita el bloqueo de su puerta desde la hora de cierre del establecimiento hasta la primera hora del día siguiente hábil.

b) Sistema de apertura automática retardada, que deberá estar activada durante la jornada laboral, salvo las cámaras de compartimentos de alquiler, que habrán de disponer de sistema electrónico de detección de ataques conectado las veinticuatro horas.

En los supuestos en que las cámaras acorazadas, con la finalidad de permitir el acceso a su interior en caso de emergencia, cuenten con trampones, éstos podrán estar libres de cualquier dispositivo de bloqueo o temporización, siempre que sus llaves sean depositadas para su custodia en otra sucursal próxima de la misma entidad o grupo.

c) Detectores sísmicos, detectores microfónicos u otros dispositivos que permitan detectar cualquier ataque a través de techos, paredes o suelo de las cámaras acorazadas o de las cajas de alquiler.

d) Detectores volumétricos.

e) Mirillas ojo de pez o dispositivos similares, o circuito cerrado de televisión en su interior, conectado con la detección volumétrica o provisto de videosensor, con proyección de imágenes en un monitor visible desde el exterior.

Estas imágenes deberán ser transmitidas a la central de alarmas o, en caso contrario, la entidad habrá de disponer del servicio de custodia de llaves para la respuesta a las alarmas.

Artículo 122. *Cajas fuertes, dispensadores de efectivo y cajeros automáticos.*

1. Las cajas fuertes deberán tener los niveles de resistencia que determine el Ministerio del Interior, y estarán protegidas con los dispositivos de bloqueo y apertura automática retardada, de acuerdo con lo dispuesto en el artículo anterior. Cuando su peso sea inferior a 2.000 kilogramos, estarán, además, ancladas, de manera fija, en estructuras de hormigón armado, al suelo o al muro.

2. Para el funcionamiento del establecimiento u oficina, las cajas auxiliares, además del cajón donde se deposita, en su caso, el efectivo necesario para realizar las operaciones, estarán provistas de elementos con posibilidad de depósito de efectivo en su interior, de forma que quede sometido necesariamente a apertura retardada para su extracción.

3. Los dispensadores de efectivo habrán de estar construidos con materiales de la resistencia que determine el Ministerio del Interior, debiendo estar conectados a la central de alarmas durante el horario de atención al público.

A estos efectos, se consideran dispensadores de efectivo los que, estando provistos de sistema de apertura automática retardada y posibilidad para admitir ingresos, permitan la dispensación automática de efectivo contra cuentas corrientes, contables o libretas de ahorro, libremente, hasta la cantidad que determine el Ministerio del Interior.

Cuando en un establecimiento u oficina todas las cajas auxiliares sean sustituidas por dispensadores de efectivo, no serán precisas las instalaciones a que se refiere el artículo 120.1.d) y e) de este Reglamento. No obstante, podrá disponerse de cajas auxiliares para su utilización en caso de avería de los dispensadores de efectivo.

4. Los cajeros automáticos deberán estar protegidos con las siguientes medidas de seguridad:

1.º Cuando se instalen en el vestíbulo del establecimiento:

a) Puerta de acceso blindada con acristalamiento resistente al menos al impacto manual del nivel que se determine, y dispositivo interno de bloqueo.

b) Dispositivo de apertura automática retardada en la puerta de acceso al depósito de efectivo, que podrá ser desactivado, durante las operaciones de carga, por los vigilantes de seguridad encargados de dichas operaciones, previo aviso, en su caso, al responsable del control de los sistemas de seguridad.

c) Detector sísmico en la parte posterior.

2.º Cuando se instalen en fachada o dentro del perímetro interior de un inmueble, las medidas establecidas en los párrafos b) y c) anteriores.

3.º Cuando se instalen en el interior de edificios, locales o inmuebles, siempre que éstos se encuentren dotados de vigilancia permanente con armas, los cajeros automáticos quedan exceptuados del cumplimiento de las anteriores medidas de seguridad, y únicamente se exigirá que estén anclados al suelo o al muro cuando su peso sea inferior a 2.000 kilogramos.

5. Si los cajeros automáticos se instalaran en espacios abiertos, y no formaran parte del perímetro de un edificio, deberán disponer de cabina anclada al suelo, de las características que se determinen, y estar protegidos con las medidas a que se refiere el apartado 1.o anterior.

Artículo 123. *Planos de planta.*

Los Bancos, Cajas de Ahorro y demás entidades de crédito mantendrán en las oficinas centrales los planos de planta actualizados de todas sus oficinas, descriptivos de la distribución de las distintas dependencias y de las instalaciones de seguridad de los diferentes servicios, e informes técnicos sobre la naturaleza de los materiales utilizados en su construcción. A requerimiento de las unidades de las Fuerzas y Cuerpos de Seguridad, les facilitarán copia de dichos planos por el procedimiento más rápido disponible.

Artículo 124. *Oficinas de cambio de divisas y módulos transportables.*

1. Los establecimientos u oficinas pertenecientes a entidades de crédito u otras mercantiles, dedicadas exclusivamente al cambio de divisas, estacional o permanentemente, dispondrán como mínimo de las medidas de seguridad previstas en el artículo 132 de este Reglamento para las Administraciones de Loterías y Apuestas Mutuas.

2. Los bancos móviles o módulos transportables, utilizados por las entidades de crédito como establecimientos u oficinas, deberán reunir, al menos, las siguientes medidas de seguridad:

a) Protección de la zona destinada al recinto de caja y puertas de acceso con blindaje de cristal antibala de la categoría y nivel que se determinen, para evitar el ataque al personal que se encuentre en el interior de dicho recinto.

El recinto de caja permanecerá cerrado desde su interior, durante las horas de atención al público, siempre que el personal se encuentre dentro del mismo.

b) Caja fuerte con dispositivo automático de retardo y bloqueo, que deberá estar fijada a la estructura del vehículo del módulo. La caja auxiliar estará provista de cajón de depósito y unida a otro de apertura retardada.

c) Señal luminosa exterior y pulsadores de la misma en el interior.

d) Carteles anunciadores como los previstos en el párrafo f) del artículo 120 de este Reglamento.

e) Servicio propio de vigilantes de seguridad, en el supuesto de que no se cuente con servicio de vigilancia de las Fuerzas y Cuerpos de Seguridad o con servicio de vigilantes de seguridad del inmueble o recinto en que se ubiquen.

3. La autorización de cada unidad o módulo para el funcionamiento de estos establecimientos u oficinas corresponderá al Director general de la Policía o al Gobernador Civil de la provincia, según que el ámbito territorial de actuación sea supraprovincial o provincial, debiendo seguirse el procedimiento regulado en el artículo 136 de este Reglamento. Una copia de la autorización deberá estar depositada en la correspondiente unidad o módulo.

Artículo 125. *Exenciones.*

La Dirección General de la Policía para supuestos que excedan del territorio de una provincia o, en otro caso, el Gobierno Civil podrán eximir a las entidades a que se refiere esta Sección de todas o alguna de las medidas de seguridad que se establecen en los artículos 120 y, en su caso, en el 121, 122 y 124, apartados 1 y 2, a solicitud de la entidad interesada, valorando las circunstancias a que se refiere el artículo 112.1, todos del presente Reglamento. A tal efecto, el órgano competente recabará el parecer de la representación de los trabajadores.

Artículo 126. *Caja Postal.*

Las normas contenidas en la presente Sección para las entidades de crédito obligarán a la sede y oficinas de la Caja Postal, pero no a las oficinas cuya principal actividad sea la prestación de los servicios públicos de Correos y Telégrafos.

Sección 2.ª Joyerías, platerías, galerías de arte y tiendas de antigüedades

Artículo 127. *Medidas de seguridad aplicables.*

1. En los establecimientos de joyería y platería, así como en aquellos otros en los que se fabriquen o exhiban objetos de tal industria, deberán instalarse, por empresas especializadas y, en su caso, autorizadas, las siguientes medidas de seguridad:

a) Caja fuerte o cámara acorazada, con el nivel de resistencia que determine el Ministerio de Justicia e Interior, para la custodia de efectivo y de objetos preciosos, dotada de sistema de apertura automática retardada, que deberá estar activado durante la jornada laboral, y dispositivo mecánico o electrónico que permita el bloqueo de la puerta, desde la hora de cierre hasta primera hora del día siguiente hábil.

Cuando la caja fuerte tenga un peso inferior a 2.000 kilogramos, deberá estar anclada, de manera fija, en una estructura de hormigón armado, al suelo o al muro.

b) Pulsadores antiatraco u otros medios de accionamiento del sistema de alarma que estarán instalados en lugares estratégicos.

c) Rejas en huecos que den a patios y pasos interiores del inmueble, así como cierres metálicos en el exterior, sin perjuicio del cumplimiento de las condiciones exigidas por las normas de lucha contra incendios.

d) Puerta blindada, con resistencia al impacto manual del nivel que se determine, en todos los accesos al interior del establecimiento, provista de los cercos adecuados y cerraduras de seguridad.

e) Protección electrónica de escaparates, ventanas, puertas y cierres metálicos.

f) Dispositivos electrónicos con capacidad para la detección redundante de la intrusión en las dependencias del establecimiento en que haya efectivo u objetos preciosos.

g) Detectores sísmicos en paredes, techos y suelos de la cámara acorazada o del local en que esté situada la caja fuerte.

h) Conexión del sistema de seguridad con una central de alarmas.

i) Carteles, del tamaño que se determine por el Ministerio de Justicia e Interior, u otros sistemas de información de análoga eficacia, para su perfecta lectura desde el exterior del establecimiento, en los que se haga saber al público las medidas de seguridad que éste posea.

2. Los establecimientos de nueva apertura deberán instalar cristales blindados, del nivel que se determine, en escaparates en los que se expongan objetos preciosos, cuyo valor en conjunto sea superior a 15.000.000 de pesetas. Esta protección también será obligatoria para las ventanas o huecos que den al exterior.

3. Las galerías de arte, tiendas de antigüedades y establecimientos que se dediquen habitualmente a la exhibición o subasta de objetos de joyería o platería, así como de antigüedades u obras de arte, cuyas obras u objetos superen en conjunto el valor que se determine, deberán adoptar las medidas de seguridad que se establecen bajo los párrafos b), c), d), e), f), h) e i) del apartado 1 de este artículo y, además, proteger con detectores sísmicos el techo y el suelo del establecimiento y las paredes medianeras con otros locales o viviendas, así como con acristalamiento blindado del nivel que se fija en el apartado anterior los escaparates de los establecimientos de nueva apertura en que se exhiban objetos por la cuantía en el mismo determinada.

Artículo 128. *Exhibiciones o subastas ocasionales.*

1. Con independencia del cumplimiento de las normas aplicables, las personas o entidades que pretendan exhibir o subastar públicamente objetos de joyería o platería, así como antigüedades u obras de arte, en locales o establecimientos no dedicados habitualmente a estas actividades deberán comunicarlo, con una antelación no inferior a quince días, al Gobernador Civil de la provincia donde vaya a efectuarse la exhibición o subasta.

2. Atendiendo a las circunstancias que concurran en cada caso y a los informes recabados, el Gobernador Civil podrá ordenar a los organizadores la adopción, con carácter previo a las exhibiciones o subastas, de las medidas de vigilancia y seguridad que considere adecuadas.

Artículo 129. *Dispensas.*

1. Teniendo en cuenta el reducido volumen de negocio u otras circunstancias que habrán de ser debidamente acreditadas, los Gobernadores Civiles podrán dispensar de todas o algunas de las medidas de seguridad previstas en el artículo 127 de este Reglamento a los establecimientos cuyos titulares lo soliciten.

2. Si lo estimasen conveniente, dichas autoridades podrán recabar la opinión al respecto de las correspondientes asociaciones empresariales de la provincia y de la representación de los trabajadores.

Sección 3.ª Estaciones de servicio y unidades de suministro de combustibles y carburantes

Artículo 130. *Enumeración de medidas de seguridad.*

1. Las estaciones de servicio y unidades de suministro de combustibles y carburantes dispondrán de una caja fuerte con el nivel de resistencia que determine el Ministerio de Justicia e Interior, con sistema o mecanismo que impida la extracción del dinero a través de

la abertura destinada a su introducción en la caja, y dos cerraduras protegidas. La caja estará empotrada en una estructura de hormigón armado, preferentemente en el suelo.

2. Una de las llaves de la caja fuerte estará en poder del encargado del negocio u otro empleado y la otra en posesión del propietario o persona responsable de la recogida de los fondos, sin que en ningún caso pueda coincidir la custodia de ambas llaves en la misma persona, ni en personas que trabajen juntas.

3. A fin de permitir las devoluciones y cambios necesarios, cada empleado de las estaciones de servicio y unidades de suministro de combustibles y carburantes sólo podrá tener en su poder, o, en el caso de autoservicio, en la caja registradora, la cantidad de dinero que fije el Ministerio de Justicia e Interior.

4. Las estaciones y unidades de suministro podrán disponer, advirtiéndolo al público usuario mediante carteles situados en lugares visibles, que sólo se despachará combustible por cantidades determinadas de dinero, de forma que puedan ser abonadas por su importe exacto sin necesidad de efectuar cambios.

5. En los casos en los que el volumen económico, la ubicación de las estaciones de servicio o, en general, su vulnerabilidad lo requiera, los Gobernadores Civiles podrán imponer la obligación de las empresas titulares de adoptar alguno de los servicios o sistemas de seguridad establecidos en el artículo 112 de este Reglamento.

6. Será de aplicación a las estaciones de servicio y unidades de suministro de combustibles y carburantes lo dispuesto sobre dispensas en el artículo 129.1 de este Reglamento.

Sección 4.ª Oficinas de farmacia, Administraciones de Lotería, Despachos de Apuestas Mutuas y establecimientos de juego

Artículo 131. *Oficinas de farmacia.*

1. Todas las oficinas de farmacia deberán contar con un dispositivo de tipo túnel, bandeja de vaivén o bandeja giratoria con seguro, que permita adecuadamente las dispensaciones a los clientes sin necesidad de que éstos penetren en el interior.

2. La utilización de esta medida será obligatoria únicamente cuando las farmacias presten servicio nocturno o de urgencia.

Artículo 132. *Administraciones de Lotería y Despachos de Apuestas Mutuas.*

1. Las Administraciones de Lotería y los Despachos Integrales de Apuestas Mutuas Deportivo-Benéficas dispondrán de un recinto cerrado en el que existirá una caja fuerte de las características determinadas en el artículo 127.1.a) del presente Reglamento en la que se custodiarán los efectos y el dinero en metálico.

2. La parte del recinto destinada al público estará totalmente separada, por elementos o materiales de blindaje del nivel que se determine, de la zona reservada a los empleados que realicen transacciones con el público, la cual estará permanentemente cerrada desde su interior y dotada de dispositivos que impidan el ataque a dichos empleados.

3. Las transacciones con el público se harán a través de ventanillas con cualquiera de los dispositivos enumerados en el apartado 1 del artículo anterior.

4. Independientemente de las mencionadas medidas de seguridad, el Gobernador Civil de la provincia, en los casos a que se refiere el artículo 130.5 de este Reglamento, podrá obligar a los titulares de estos establecimientos a la adopción de los sistemas de seguridad a que se refieren los párrafos c) y d) del artículo 112, también del presente Reglamento.

Artículo 133. *Locales de juegos de azar.*

1. Las medidas de seguridad establecidas en los apartados 1 y 2 del artículo anterior serán aplicables asimismo a los casinos de juego.

2. A las salas de bingo autorizadas para más de ciento cincuenta jugadores, así como a los salones de máquinas de juego autorizados para más de setenta y cinco máquinas de juego, les será de aplicación la medida de seguridad regulada en los apartados 1 y 2 del artículo 130 de este Reglamento.

Artículo 134. *Dispensas.*

Será de aplicación a esta sección lo dispuesto sobre dispensas en el artículo 129 del presente Reglamento.

Sección 5.ª Mantenimiento de las medidas de seguridad

Artículo 135. *Revisión. Libro-catálogo.*

1. A los efectos de mantener el funcionamiento de las distintas medidas de seguridad previstas en el presente título y de la consecución de la finalidad preventiva y protectora, propia de cada una de ellas, la dirección de cada entidad o establecimiento obligado a tener medidas de seguridad electrónicas dispondrá la revisión y puesta a punto, trimestralmente, de dichas medidas por personal especializado de empresas de seguridad, o propio si dispone de medios adecuados, no debiendo transcurrir más de cuatro meses entre dos revisiones sucesivas, y anotará las revisiones y puestas a punto que se realicen en un libro-catálogo de las instaladas según el modelo que se apruebe con arreglo a las normas que dicte el Ministerio de Justicia e Interior, concebido de forma que pueda ser objeto de tratamiento y archivo mecanizado e informatizado.

Este libro-catálogo será también obligatorio para las empresas industriales, comerciales o de servicios, conectadas a centrales de alarmas.

2. Cuando las instalaciones permitan la comprobación del estado y del funcionamiento de cada uno de los elementos del sistema desde la central de alarmas, las revisiones preventivas tendrán una periodicidad anual, no pudiendo transcurrir más de catorce meses entre dos sucesivas.

CAPITULO III

Apertura de establecimientos u oficinas obligados a disponer de medidas de seguridad

Artículo 136. *Autorización.*

1. Cuando se pretenda la apertura o traslado de un establecimiento u oficina, cuyos locales o instalaciones hayan de disponer, en todos o algunos de sus servicios, de medidas de seguridad determinadas en este Reglamento, el responsable de aquéllos solicitará la autorización del Delegado del Gobierno, el cual ordenará el examen y comprobación de las medidas de seguridad instaladas y su correcto funcionamiento, a los funcionarios que tienen atribuidas legalmente dichas facultades. Hasta tanto tal comprobación tenga lugar, podrá autorizarse provisionalmente, por la autoridad policial competente, la apertura del establecimiento u oficina por un plazo máximo de tres meses, siempre que se implante transitoriamente el servicio de vigilantes de seguridad con armas.

Cuando se trate de la reforma de un establecimiento u oficina, anteriormente autorizados, que implique la adopción o modificación de medidas de seguridad, bastará la comunicación a las dependencias policiales competentes, para su comprobación.

2. Practicada la inspección sin constatar deficiencias de las medidas de seguridad obligatorias, el establecimiento podrá continuar con sus actividades sin necesidad del servicio de vigilancia armada, hasta que tenga lugar la autorización definitiva, o bien proceder a la apertura provisional, si no lo hubiera hecho con anterioridad, bastando para ello el acta favorable de inspección.

3. De observarse deficiencias en las medidas de seguridad obligatorias, se entregará copia del acta de inspección a la empresa o entidad interesada para la subsanación de aquéllas en el plazo máximo de un mes, debiendo comunicarse la subsanación a la dependencia policial competente a efectos de nueva comprobación. Durante el indicado plazo, el establecimiento podrá permanecer en funcionamiento siempre que cuente con el servicio de vigilantes de seguridad con armas.

Transcurrido dicho plazo sin que la empresa o entidad interesada haya comunicado la subsanación de las deficiencias, se procederá al cierre del establecimiento u oficina hasta

que se constate la subsanación de las mismas mediante la correspondiente acta de inspección.

4. En el caso de que la empresa o entidad solicitante no recibiere indicación o comunicación alguna, en el plazo de tres meses siguientes a la fecha de presentación de la solicitud de autorización, o en el de un mes desde la fecha de presentación de la comunicación relativa a la subsanación de deficiencias, podrá entender autorizada la apertura o traslado del establecimiento o aprobada la reforma efectuada.

5. Las medidas de seguridad no obligatorias y las reformas que no afecten a los elementos esenciales del sistema de seguridad, instalados en este tipo de establecimientos u oficinas, habrán de ser comunicadas a las dependencias policiales de los órganos competentes, antes de su entrada en funcionamiento, pero no estarán sujetas a autorización previa.

6. Las previsiones contenidas en el presente artículo serán también aplicables a los cajeros automáticos, en los supuestos de instalación y entrada en funcionamiento, modificación o traslado de los mismos.

TITULO IV

Control e inspección

CAPITULO I

Información y control

Artículo 137. *Competencias y funciones.*

1. Corresponde el ejercicio de la competencia de control para el cumplimiento de la Ley 23/1992, de 30 de julio, de Seguridad Privada, al Ministerio de Justicia e Interior y a los Gobernadores Civiles.

2. Corresponde al Cuerpo Nacional de Policía y, en su caso, al de la Guardia Civil, el cumplimiento de las órdenes e instrucciones que se impartan por los órganos indicados, en el ejercicio de la función de control de las entidades, servicios o actuaciones y del personal y medios en materia de seguridad privada, vigilancia e investigación.

3. Sin perjuicio de lo dispuesto en el apartado anterior, el ejercicio de la función de control de las actuaciones de los guardas particulares del campo, en sus distintas modalidades, corresponde especialmente a la Dirección General de la Guardia Civil.

4. Para el ejercicio de las competencias respectivamente atribuidas por la legislación de seguridad privada a las Direcciones Generales de la Policía y de la Guardia Civil, éstas llevarán ficheros automatizados, destinados a registrar las infracciones cometidas y las sanciones impuestas en los procedimientos sancionadores en que hubieran intervenido en la materia.

Artículo 138. *Documentación anual.*

1. Durante el primer trimestre de cada año, todas las empresas de seguridad remitirán a la Secretaría de Estado de Interior un informe explicativo de las actividades realizadas en el año anterior, en el que constará:

a) La relación de altas y bajas producidas en el personal de seguridad, con indicación de los datos consignados en el correspondiente libro-registro.

b) La relación de servicios realizados, con indicación del nombre de la entidad o persona a la que se prestaron y especificación de la naturaleza de los servicios, determinada con arreglo a la enumeración contenida en el artículo 1 de este Reglamento.

c) El resumen de las comunicaciones efectuadas a las Fuerzas y Cuerpos de Seguridad en relación con la seguridad ciudadana.

d) La relación de auxilios, colaboraciones y entregas de detenidos a las Fuerzas y Cuerpos de Seguridad.

2. Asimismo, las empresas de seguridad remitirán a la Secretaría de Estado de Interior, durante el primer semestre de cada año, el resumen de la cuenta anual, en el que se refleje la situación patrimonial y financiera de la empresa.

Artículo 139. *Comunicación sobre la vigencia del contrato de seguro, aval u otra garantía financiera suscrita para cubrir la responsabilidad.*

1. Anualmente, en el mismo plazo determinado en el apartado 1 del artículo anterior, las empresas de seguridad habrán de presentar, en el registro en que se encontraran inscritas, certificado acreditativo de vigencia del contrato de seguro, aval u otra garantía financiera que hubieran suscrito para cubrir la responsabilidad.

2. La empresa asegurada tiene la obligación de comunicar a la Dirección General de la Policía y de la Guardia Civil (ámbito del Cuerpo Nacional de Policía), la rescisión y cualquiera otra de las circunstancias que puedan dar lugar a la terminación del contrato de seguro de responsabilidad civil, aval u otra garantía financiera, al menos con treinta días de antelación a la fecha en que dichas circunstancias hayan de surtir efecto.

3. En todos los supuestos de terminación de la vigencia del contrato de seguro, aval u otra garantía financiera, la empresa deberá concertar oportunamente, de forma que no se produzca solución de continuidad en la cobertura de la responsabilidad, nueva póliza de responsabilidad civil, aval u otra garantía financiera, que cumpla las exigencias establecidas en el artículo 5.1.c).6.º y en el anexo de este reglamento, acreditándolo ante el Registro de Empresas de Seguridad.

Artículo 140. *Comunicación de modificaciones estatutarias.*

1. Cuando las empresas de seguridad revistan la forma de persona jurídica estarán obligadas a comunicar a la Secretaría de Estado de Seguridad todo cambio que se produzca en la titularidad de las acciones, participaciones o aportaciones y los que afecten a su capital social, dentro de los quince días siguientes a su modificación.

2. Asimismo, y en igual plazo, deberán comunicar cualquier modificación de sus Estatutos y toda variación que sobrevenga en la composición personal de sus órganos de administración y dirección.

3. Las comunicaciones a que se refieren los apartados anteriores deberán efectuarse mediante copia autorizada de la correspondiente escritura pública o del documento en que se hubieren consignado las modificaciones.

4. Cuando los cambios implicaran la pérdida de los requisitos de los administradores y directores de las empresas de seguridad, cesarán en sus cargos.

Artículo 141. *Memoria anual de los detectives privados.*

Los detectives privados habrán de presentar en la Secretaría de Estado de Seguridad, dentro del primer trimestre de cada año, una memoria de actividades del año precedente, en la que se hará constar la relación de servicios efectuados, la condición física o jurídica de las personas con las que se concertaron, consignándose en este último caso el sector específico y la actividad concreta de que se trate, la naturaleza de los servicios prestados, los hechos delictivos perseguibles de oficio comunicados como consecuencia de su actuación, y los órganos gubernativos a los que se comunicaron.

Artículo 142. *Perfeccionamiento del sector.*

1. Teniendo en cuenta la información reunida anualmente a través del cumplimiento de lo dispuesto en los artículos anteriores y en los restantes del presente Reglamento, el Ministerio de Justicia e Interior:

a) Dará cuenta anualmente al Gobierno y a las Cortes Generales sobre el funcionamiento del sector de la seguridad privada.

b) Adoptará o promoverá las medidas de carácter general adecuadas para perfeccionar dicho funcionamiento y para asegurar la consecución de las finalidades de la Ley 23/1992, de 30 de julio, de Seguridad Privada.

2. Corresponde al Ministerio de Justicia e Interior, a través de la Dirección General de la Policía, la planificación, información, asesoramiento y coordinación de la seguridad de las personas, edificios, instalaciones, actividades y objetos de especial interés, en el ámbito de la Administración General del Estado y de las entidades de Derecho Público vinculadas o dependientes de ella.

CAPITULO II

Inspección

Artículo 143. *Acceso de los funcionarios.*

1. Los libros-registro de las empresas de seguridad y de los detectives privados determinados en el presente Reglamento estarán a disposición de los miembros del Cuerpo Nacional de Policía, encargados de su control, para las inspecciones que deban realizar.

2. Las empresas y el personal de seguridad privada de las mismas facilitarán el acceso de los funcionarios de las Fuerzas y Cuerpos de Seguridad competentes a los armeros, al objeto de que puedan realizar las comprobaciones pertinentes sobre los propios armeros y las armas que contengan.

3. Las empresas de depósito, custodia, recuento y clasificación de monedas y billetes, títulos-valores y objetos valiosos o peligrosos facilitarán la inspección de la cámara acorazada con el fin de hacer las pertinentes comprobaciones de los datos que figuren en los libros-registro.

4. Del mismo modo, las empresas, entidades y organismos que deban tener instalados dispositivos, sistemas o medidas de seguridad, o que tengan servicios de protección prestados por personal de seguridad, o sistemas de seguridad conectados a centrales de alarma, deberán facilitar el acceso a los miembros de las Fuerzas y Cuerpos de Seguridad encargados de las funciones inspectoras a que se refiere este Reglamento, con objeto de que puedan comprobar en cualquier momento el estado de las instalaciones y su funcionamiento.

Artículo 144. *Inspecciones.*

1. Aparte del desarrollo de los planes de inspección que tengan establecidos, cuando recibieren denuncias sobre irregularidades cometidas por empresas o personal de seguridad, o por centros de formación o su personal, los servicios policiales de inspección y control procederán a la comprobación de los hechos denunciados y, en su caso, a la apertura del correspondiente procedimiento.

2. Siempre que el personal indicado realice una inspección de empresas de seguridad, de establecimientos públicos o privados, o de despachos de los detectives privados:

a) Diligenciará los libros revisados, haciendo constar las deficiencias o anomalías que observare.

b) Efectuará las comprobaciones precisas para la constatación del contenido reflejado en los libros, debiendo las empresas y el personal de seguridad colaborar con tal objeto.

c) De cada inspección, extenderá el acta correspondiente, facilitando una copia al responsable del establecimiento.

3. Los actos de inspección, que se contraerán a las medidas, medios y actividades de seguridad privada, podrán desarrollarse, indistintamente:

a) En la sede social de la empresa, delegaciones, oficinas, locales, despachos, o lugares anejos a éstos, en los que se desarrollen actividades de seguridad privada o relacionadas con ésta.

b) En los inmuebles, espacios o lugares en donde se presten servicios de seguridad privada.

CAPITULO III

Medidas cautelares

Artículo 145. *Ocupación o precinto.*

Los funcionarios policiales competentes podrán acordar, inmediata y excepcionalmente, la medida cautelar de ocupación o precinto de vehículos, armas, material o equipo prohibido, no homologado o que resulte peligroso o perjudicial, así como de los instrumentos y efectos de la infracción, en supuestos de grave riesgo o peligro inminente para las personas o bienes, debiendo, para el mantenimiento de la medida, ser ratificada por las autoridades sancionadoras competentes.

Artículo 146. *Retirada de armas.*

Con independencia de las responsabilidades penales o administrativas a que hubiere lugar, los funcionarios policiales competentes se harán cargo de las armas y darán cumplimiento a lo dispuesto en el artículo 148.2 del Reglamento de Armas, sobre depósito de las que se porten o utilicen ilegalmente, en los siguientes casos:

a) Si detectaren la prestación de servicios por personal de seguridad privada con armas, cuando debieran prestarse sin ellas.
b) Cuando el personal de seguridad privada porte armas fuera de los lugares o de las horas de servicio, sin la oportuna autorización en los casos previstos en el presente Reglamento.

Artículo 147. *Suspensión de servicios.*

Cuando los funcionarios policiales competentes observaren la prestación de servicios de seguridad privada o la utilización de medios materiales o técnicos que puedan causar daños o perjuicios a terceros o poner en peligro la seguridad ciudadana, suspenderán su prestación, debiendo tal decisión ser ratificada por el Secretario de Estado de Interior o por los Gobernadores Civiles en el plazo de setenta y dos horas.

TITULO V

Régimen sancionador

CAPITULO I

Cuadro de infracciones

Sección 1.ª Empresas de seguridad

Artículo 148. *Infracciones muy graves.*

Las empresas podrán incurrir en las siguientes infracciones muy graves:

1. La prestación de servicios de seguridad a terceros, careciendo de la autorización necesaria, incluyendo:

a) La prestación de servicios de seguridad sin haber obtenido la inscripción y la autorización de entrada en funcionamiento para la clase de servicios o actividades de que se trate.
b) La continuación de la prestación de servicios en caso de cancelación de la inscripción o de rescisión del contrato de seguro, aval u otra garantía equivalente, sin concertar otra nueva otra nueva dentro del plazo reglamentario.
c) La subcontratación de los servicios y actividades de seguridad privada con empresas que no dispongan de la correspondiente habilitación o reconocimiento necesarios para el servicio o actividad de que se trate, salvo en los supuestos reglamentariamente permitidos.

2. La realización de actividades prohibidas en el artículo 3 de la Ley, sobre conflictos políticos o laborales, control de opiniones, recogida de datos personales con tal objeto, o información a terceras personas sobre sus clientes o su personal, en el caso de que no sean constitutivas de delito.

3. La instalación de medios materiales o técnicos no homologados que sean susceptibles de causar grave daño a las personas o a los intereses generales.

4. La negativa a facilitar, cuando proceda, la información contenida en los libros registros reglamentarios.

5. El incumplimiento de las previsiones normativas sobre adquisición y uso de las armas, así como sobre disponibilidad de armeros, conservación, mantenimiento, buen funcionamiento de las armas y custodia de las mismas, particularmente la tenencia de armas por el personal a su servicio fuera de los casos permitidos por la Ley, incluyendo:

a) Poseer armas que no sean las reglamentariamente determinadas para el servicio de que se trate.

b) La tenencia de armas careciendo de la guía de pertenencia de las mismas.

c) Adjudicar al personal de seguridad armas que no sean las reglamentariamente establecidas para el servicio.

d) La negligencia en la custodia de armas, que pueda provocar su sustracción, robo o extravío.

e) Carecer de armero con la correspondiente homologación o no hacer uso del mismo, en los casos en que esté exigido en el presente Reglamento.

f) La realización de los ejercicios de tiro obligatorios por el personal de seguridad sin la presencia o sin la dirección del instructor de tiro o, en su caso, del jefe de seguridad, o incumpliendo lo dispuesto al efecto en el artículo 84.2 de este Reglamento.

g) Proveer de armas a personal que carezca de la licencia reglamentaria.

6. La realización de servicios de seguridad con armas fuera de los casos previstos en la Ley y en el presente Reglamento, así como encargar servicios con armas a personal que carezca de la licencia reglamentaria.

7. La negativa a prestar auxilio o colaboración con las Fuerzas y Cuerpos de Seguridad en la investigación y persecución de actos delictivos, en el descubrimiento y detención de los delincuentes o en la realización de las funciones inspectoras o de control que les correspondan, incluyendo:

a) La falta de comunicación oportuna a las Fuerzas y Cuerpos de Seguridad de informaciones relevantes para la prevención, mantenimiento o restablecimiento de la seguridad ciudadana.

b) La falta de comunicación oportuna de los hechos delictivos de que tuvieren conocimiento en el desarrollo de sus actividades.

c) La negativa a facilitar a los funcionarios competentes los contratos, libros-registro u hojas de ruta reglamentarios, que contengan datos relacionados con los servicios de seguridad privada.

d) La negativa a facilitar a dichos funcionarios el acceso a los lugares donde se lleven a cabo actividades de seguridad privada, o se presten servicios de esta naturaleza, excepto a los domicilios particulares.

e) Impedir o dificultar de cualquier modo el control de la prestación de servicios de seguridad, cuando se establezcan sistemas informáticos de comunicación.

8. La comisión de una tercera infracción grave en el período de un año.

Artículo 149. *Infracciones graves.*

Las empresas de seguridad podrán incurrir en las siguientes infracciones graves:

1. La instalación de medios materiales o técnicos no homologados, cuando la homologación sea preceptiva.

2. La realización de servicios de transportes con vehículos que no reúnan las características reglamentarias, incluyendo:

a) La utilización de vehículos con distintivos o características semejantes a los de las Fuerzas Armadas o a los de las Fuerzas y Cuerpos de Seguridad o con lanzadestellos o sistemas acústicos que les estén prohibidos.

b) La realización de los servicios de transporte o distribución sin que los vehículos cuenten con la dotación reglamentaria de vigilantes de seguridad o, en su caso, sin la protección necesaria.

3. La realización de funciones que excedan de la habilitación obtenida o reconocida por la empresa de seguridad o por el personal a su servicio, o fuera del lugar o ámbito territorial correspondiente, así como la retención de la documentación personal; la realización de servicios en polígonos industriales y urbanizaciones sin haber obtenido la autorización expresa de la Delegación o Subdelegación del Gobierno o del órgano correspondiente de la comunidad autónoma competente, y la subcontratación de servicios de seguridad con empresas inscritas, pero no habilitadas o reconocidas para el ámbito territorial correspondiente al lugar de realización del servicio o actividad subcontratados.

4. La realización de los servicios de seguridad sin formalizar o sin comunicar a la autoridad competente la celebración de los correspondientes contratos, incluyendo:

a) La realización de servicios de protección personal, careciendo de la autorización a que se refieren los artículos 27 y siguientes de este Reglamento, fuera del plazo establecido o al margen de las condiciones impuestas en la autorización.

b) La falta de comunicación de los contratos, o, en su caso, de las ofertas en que se concreten sus prestaciones, o de las modificaciones de los mismos, a las autoridades competentes ; no hacerlo dentro de los plazos establecidos, o realizarlo sin ajustarse a los modelos o formatos aprobados, y la prestación de los servicios, en circunstancias o condiciones distintas de las previstas en los contratos comunicados.

c) La falta de comunicación a las autoridades competentes, dentro del plazo establecido, de la prestación de servicios urgentes, en circunstancias excepcionales.

5. La utilización en el ejercicio de funciones de seguridad, de personas que carezcan de la nacionalidad, cualificación, acreditación o titulación exigidas, o de cualquier otro de los requisitos necesarios, **incluyendo el de la superación de los correspondientes cursos de actualización y especialización con la periodicidad establecida**, y la utilización de personal habilitado sin la correspondiente comunicación de alta en las empresas, en la forma establecida.

6. El abandono o la omisión injustificados del servicio, dentro de la jornada laboral establecida, por parte de los vigilantes de seguridad y de todo el personal de seguridad privada al que se aplican las normas de los vigilantes.

7. La falta de presentación a la autoridad competente del informe anual de actividades, en la forma y plazo prevenidos o con omisión de las informaciones requeridas legal y reglamentariamente.

8. No transmitir a las Fuerzas y Cuerpos de Seguridad las señales de alarma que se registren en las centrales privadas, transmitir las señales con retraso injustificado o comunicar falsas incidencias, por negligencia, deficiente funcionamiento o falta de verificación previa, incluyendo:

a) El funcionamiento deficiente de las centrales de alarmas por carecer del personal preciso.

b) La transmisión de alarmas a los servicios policiales sin verificarlas previa y adecuadamente.

c) La transmisión de falsas alarmas a las Fuerzas y Cuerpos de Seguridad por falta de adopción de las precauciones necesarias para evitarlas.

d) La falta de subsanación de las deficiencias que den lugar a falsas alarmas, cuando se hubiere sido requerido para ello, y la de desconexión del sistema que hubiere sido reglamentariamente ordenada.

9. La comisión de una tercera infracción leve en el período de un año.

Téngase en cuenta que se anula el inciso destacado en el apartado 5 por Sentencia del TS de 15 de enero de 2009. Ref. BOE-A-2009-3500.

Artículo 150. *Infracciones leves.*

Las empresas de seguridad podrán incurrir en las siguientes infracciones leves:

1. La entrada en funcionamiento de las empresas de seguridad sin dar cuenta de ello a los servicios policiales competentes, salvo que constituya infracción grave o muy grave.
2. La apertura de delegaciones o sucursales sin obtener la autorización necesaria del órgano competente.
3. La omisión del deber de abrir sucursales o delegaciones en los supuestos prevenidos en los apartados 2 y 3 del artículo 17.
4. La publicidad de la empresa sin estar inscrita y autorizada, y la realización de publicidad de las actividades y servicios o la utilización de documentos o impresos en sus comunicaciones, sin hacer constar el número de registro de la empresa.
5. La falta de presentación anual, dentro del plazo establecido, del certificado acreditativo de la vigencia del contrato de seguro, aval u otra garantía equivalente.
6. La falta de comunicación a la autoridad competente, en el plazo y en la forma prevenidos, de los cambios que afecten a la titularidad de las acciones o participaciones en el capital o a la composición personal de los órganos de administración, y de cualquier variación en los órganos de dirección de la sociedad.
7. La falta de comunicación a la autoridad competente de la información prevenida durante la prestación de servicios de protección personal o la relativa a la finalización del servicio.
8. La omisión del deber de reserva en la programación, itinerario y realización de los servicios relativos al transporte y distribución de objetos valiosos o peligrosos.
9. La realización de las operaciones de transporte, carga o descarga de objetos valiosos o peligrosos en forma distinta de la prevenida o sin adoptar las precauciones necesarias para su seguridad.
10. La realización de los servicios sin asegurar la comunicación entre la sede de la empresa y el personal que los desempeñe cuando fuere obligatoria.
11. La omisión de las prevenciones o precauciones reglamentarias en el transporte de objetos valiosos por vía marítima o aérea.
12. La omisión de los proyectos de instalación, previos a la instalación de medidas de seguridad; de las comprobaciones necesarias, o de la expedición del correspondiente certificado que garantice que las instalaciones de seguridad cumplen las exigencias reglamentarias.
13. La falta de realización de las revisiones obligatorias de las instalaciones de seguridad sin cumplir la periodicidad establecida o con personal que no reúna la cualificación requerida.
14. La carencia de servicio técnico necesario para arreglar las averías que se produzcan en los aparatos, dispositivos o sistemas de seguridad obligatorios; o tenerlo sin la capacidad o eficacia adecuadas.
15. El incumplimiento de la obligación de entregar el manual de la instalación o el manual de uso del sistema de seguridad o facilitarlos sin reunir las exigencias reglamentarias.
16. La prestación de servicios de custodia de llaves, careciendo de armero o de caja fuerte o sin cumplir las precauciones prevenidas al efecto.
17. La actuación del personal de seguridad sin la debida uniformidad o los medios que reglamentariamente sean exigibles.
18. La omisión del deber de adaptar los libros-registro reglamentarios a las normas reguladoras de sus formatos o modelos ; del de llevarlos regularmente y al día, o del de cumplir las normas de funcionamiento del sistema o sistemas de información, comunicación o certificación que se determinen.

19. En general, el incumplimiento de los trámites, condiciones o formalidades establecidos por la Ley de Seguridad Privada o por el presente Reglamento, siempre que no constituya delito o infracción grave o muy grave.

Sección 2.ª Personal de seguridad privada

Artículo 151. *Infracciones muy graves.*

El personal que desempeñe funciones de seguridad privada, podrá incurrir en las siguientes infracciones muy graves:

1. La prestación de servicios de seguridad a terceros por parte de personal no integrado en empresas de seguridad, careciendo de la habilitación necesaria, lo que incluye:

a) Prestar servicios de seguridad privada sin haber obtenido la tarjeta de identidad profesional correspondiente o sin estar inscrito, cuando proceda, en el pertinente registro.
b) Ejercer funciones de seguridad privada distintas de aquellas para las que se estuviere habilitado.
c) Abrir despachos de detective privado o dar comienzo a sus actividades sin estar inscrito en el reglamentario registro o careciendo de la tarjeta de identidad profesional.
d) Prestar servicios como detective asociado o dependiente sin estar inscrito en el correspondiente registro o sin tener la tarjeta de identidad profesional.
e) La utilización por los detectives privados de los servicios de personal no habilitado para el ejercicio de funciones de investigación.

2. El incumplimiento de las previsiones contenidas en la Ley 23/1992, de 30 de julio, de Seguridad Privada, y en el presente Reglamento sobre tenencia de armas fuera del servicio y sobre su utilización, incluyendo:

a) La prestación con armas de servicios de seguridad para los que no estuviese legal o reglamentariamente previsto su uso.
b) Portar sin autorización específica las armas fuera de las horas o de los lugares de prestación de los servicios o no depositarlas en los armeros correspondientes.
c) Descuidar la custodia de sus armas o de las documentaciones de éstas, dando lugar a su extravío, robo o sustracción.
d) No comunicar oportunamente a las Fuerzas y Cuerpos de Seguridad el extravío, destrucción, robo o sustracción del arma asignada.
e) Prestar con arma distinta de la reglamentaria los servicios que puedan ser realizados con armas.
f) Retener las armas o sus documentaciones cuando causaren baja en la empresa a la que pertenecieren.

3. La falta de reserva debida sobre las investigaciones que realicen los detectives privados o la utilización de medios materiales o técnicos que atenten contra el derecho el honor, a la intimidad personal o familiar, a la propia imagen o al secreto de las comunicaciones, incluyendo la facilitación de datos sobre las investigaciones que realicen a personas distintas de las que se las encomienden.
4. La condena mediante sentencia firme por un delito doloso cometido en el ejercicio de sus funciones.
5. La negativa a prestar auxilio o colaboración con las Fuerzas y Cuerpos de Seguridad, cuando sea procedente, en la investigación y persecución de actos delictivos, en el descubrimiento y detención de los delincuentes o en la realización de las funciones inspectoras o de control que les correspondan, incluyendo:

a) La falta de comunicación a las Fuerzas y Cuerpos de Seguridad de informaciones relevantes para la seguridad ciudadana, así como de los hechos delictivos de que tuvieren conocimiento en el ejercicio de sus funciones.
b) Omitir la colaboración que sea requerida por las Fuerzas y Cuerpos de Seguridad en casos de suspensión de espectáculos, desalojo o cierre de locales y en cualquier otra situación en que sea necesaria para el mantenimiento o el restablecimiento de la seguridad ciudadana.

c) La omisión del deber de realizar las identificaciones pertinentes, cuando observaren la comisión de delitos, o del de poner a disposición de las Fuerzas y Cuerpos de Seguridad a sus autores o a los instrumentos o pruebas de los mismos.

d) No facilitar a la Administración de Justicia o a las Fuerzas y Cuerpos de Seguridad las informaciones de que dispusiesen y que les fueren requeridas en relación con las investigaciones que estuviesen realizando.

6. La comisión de una tercera infracción grave en el período de un año.

Artículo 152. *Infracciones graves.*

El personal que desempeñe funciones de seguridad privada podrá incurrir en las siguientes infracciones graves:

1. La realización de funciones o servicios que excedan de la habilitación obtenida, incluyendo:

a) Abrir despachos delegados o sucursales los detectives privados sin reunir los requisitos reglamentarios, sin comunicarlo a la autoridad competente o sin acompañar los documentos necesarios.

b) La realización por los detectives privados, de funciones que no les corresponden, y especialmente la investigación de delitos perseguibles de oficio.

c) Realizar los vigilantes de seguridad actividades propias de su profesión fuera de los edificios o inmuebles cuya vigilancia y protección tuvieran encomendada, salvo en los casos en que estuviere reglamentariamente prevista.

d) El desempeño de las funciones de escolta privado excediéndose de las finalidades propias de su protección o la identificación o detención de personas salvo que sea imprescindible para la consecución de dichas finalidades.

e) Simultanear, en la prestación del servicio, las funciones de seguridad privada con otras distintas, o ejercer varias funciones de seguridad privada que sean incompatibles entre sí.

2. El ejercicio abusivo de sus funciones en relación con los ciudadanos, incluyendo:

a) La comisión de abusos, arbitrariedades o violencias contra las personas.

b) La falta de proporcionalidad en la utilización de sus facultades o de los medios disponibles.

3. No cumplir, en el ejercicio de su actuación profesional, el deber de impedir o evitar prácticas abusivas, arbitrarias o discriminatorias, que entrañen violencia física o moral, en el trato a las personas.

4. La falta de respeto al honor o a la dignidad de las personas.

5. La realización de actividades prohibidas sobre conflictos políticos y laborales, control de opiniones o comunicación de información a terceros sobre sus clientes, personas relacionadas con ellos, o sobre los bienes y efectos que custodien, incluyendo:

a) El interrogatorio de los detenidos o la obtención de datos sobre los ciudadanos a efectos de control de opiniones de los mismos.

b) Facilitar a terceros información que conozcan como consecuencia del ejercicio de sus funciones.

6. El ejercicio de los derechos sindicales o laborales al margen de lo dispuesto al respecto para los servicios públicos, en los supuestos a que se refiere el artículo 15 de la Ley.

7. La falta de presentación al Ministerio de Justicia e Interior, del informe de actividades de los detectives privados, en la forma y plazo prevenidos o su presentación careciendo total o parcialmente de las informaciones necesarias.

8. La falta de denuncia a la autoridad competente de los delitos que conozcan los detectives privados en el ejercicio de sus funciones.

9. La comisión de una tercera infracción leve en el período de un año.

Artículo 153. *Infracciones leves.*

El personal que desempeñe funciones de seguridad privada podrá incurrir en las siguientes infracciones leves:

1. La actuación sin la debida uniformidad o medios que reglamentariamente sean exigibles, por parte del personal no integrado en empresas de seguridad.
2. El trato incorrecto o desconsiderado con los ciudadanos con los que se relacionen en el ejercicio de sus funciones.
3. No comunicar oportunamente al registro las variaciones de los datos registrales de los detectives titulares o detectives asociados o dependientes.
4. La publicidad de los detectives privados careciendo de la habilitación necesaria, y la realización de la publicidad o la utilización de documentos o impresos, sin hacer constar el número de inscripción en el registro.
5. No llevar los detectives privados el libro-registro prevenido, no llevarlo con arreglo a las normas reguladoras de modelos o formatos, o no hacer constar en él los datos necesarios.
6. No comunicar oportunamente a las Fuerzas y Cuerpos de Seguridad el extravío, destrucción, robo o sustracción de la documentación relativa a las armas que tuvieran asignadas.
7. La falta de comunicación oportuna por parte del personal de seguridad privada de las ausencias del servicio o de la necesidad de ausentarse, a efectos de sustitución o relevo.
8. La utilización de perros en la prestación de los servicios, sin cumplir los requisitos o sin tener en cuenta las precauciones prevenidas al efecto.
9. No utilizar los uniformes y distintivos, cuando sea obligatorio, o utilizarlos fuera de los lugares o de las horas de servicio.
10. La delegación por los jefes de seguridad de facultades no delegables o hacerlo en personas que no reúnan los requisitos reglamentarios.
11. Desatender sin causa justificada las instrucciones de las Fuerzas y Cuerpos de Seguridad en relación con las personas o bienes objeto de su vigilancia y protección.
12. No mostrar su documentación profesional a los funcionarios policiales o no identificarse ante los ciudadanos con los que se relacionasen en el servicio, si fuesen requeridos para ello.
13. En general, el incumplimiento de los trámites, condiciones o formalidades establecidos por la Ley de Seguridad Privada o por el presente Reglamento, siempre que no constituyan delito o infracción grave o muy grave, incluyendo la no realización de los correspondientes cursos de actualización y especialización o no hacerlos con la periodicidad establecida.

Sección 3.ª Usuarios de los servicios de seguridad

Artículo 154. *Infracciones.*

Las personas físicas o jurídicas, entidades y organismos que utilicen medios o contraten la prestación de servicios de seguridad podrán incurrir en las infracciones siguientes:

1. Infracciones muy graves: la utilización de aparatos de alarmas, dispositivos o sistemas de seguridad no homologados que fueren susceptibles de causar graves daños a las personas o a los interesados generales.
2. Infracciones graves:

a) La utilización de aparatos de alarma o dispositivos de seguridad que no se hallen debidamente homologados.
b) La contratación o utilización de los servicios de empresas carentes de la habilitación específica necesaria para el desarrollo de los servicios de seguridad privada, a sabiendas de que no reúnen los requisitos legales al efecto.

3. Infracciones leves:

a) La utilización de aparatos o dispositivos de seguridad sin ajustarse a las normas que los regulen o su funcionamiento con daños o molestias para terceros.

b) La instalación de marcadores automáticos para transmitir alarmas directamente a las dependencias de las Fuerzas y Cuerpos de Seguridad.

c) La contratación o utilización de personal de seguridad que carezca de la habilitación específica necesaria, a sabiendas de que no reúne los requisitos legales.

Sección 4.ª Infracciones al régimen de medidas de seguridad

Artículo 155. *Infracciones.*

1. Los titulares de las empresas, entidades y establecimientos obligados por el presente Reglamento o por decisión de la autoridad competente a la adopción de medidas de seguridad para prevenir la comisión de actos delictivos podrán incurrir en las siguientes infracciones de acuerdo con lo dispuesto en los artículos 23.n), 24 y 26.f), h) y j), de la Ley Orgánica 1/1992, de 21 de febrero, sobre Protección de la Seguridad Ciudadana:

1.º Infracciones muy graves: podrán ser consideradas infracciones muy graves las infracciones graves, teniendo en cuenta la entidad del riesgo producido o del perjuicio causado.

2.º Infracciones graves:

a) Proceder a la apertura de un establecimiento u oficina o iniciar sus actividades antes de que el órgano competente haya concedido la necesaria autorización.

b) Proceder a la apertura o ejercer las actividades propias del establecimiento u oficina antes de que las medidas de seguridad obligatorias hayan sido adoptadas y funcionen adecuadamente.

c) Mantener abierto el establecimiento u oficina sin que las medidas de seguridad reglamentariamente exigidas funcionen, o sin que lo hagan correcta y eficazmente.

3.º Infracciones leves:

a) Las irregularidades en la cumplimentación de los registros prevenidos.

b) La omisión de los datos o comunicaciones obligatorios dentro de los plazos prevenidos.

c) La desobediencia de los mandatos de la autoridad o de sus agentes, dictados en directa aplicación de lo prevenido en la Ley Orgánica 1/1992, de 21 de febrero, desarrollado, en su caso, reglamentariamente sobre medidas de seguridad en establecimientos e instalaciones, siempre que no constituya infracción penal.

d) La desobediencia de los mandatos de la autoridad o de sus agentes, dictados en aplicación de la Ley Orgánica 1/1992, de 21 de febrero, sobre Protección de la Seguridad Ciudadana, siempre que no constituya infracción penal.

2. También, de acuerdo con lo dispuesto en los artículos 23.n), 24 y 26.h) y j) de la Ley Orgánica 1/1992, de 21 de febrero, sobre Protección de la Seguridad Ciudadana, el personal de las empresas, entidades o establecimientos obligados a la adopción de medidas de seguridad para prevenir la comisión de actos delictivos, podrá incurrir en las siguientes infracciones, sin perjuicio de la responsabilidad en que incurran por los mismos hechos las empresas, entidades o establecimientos indicados:

1. Infracciones muy graves: podrán ser consideradas muy graves las infracciones graves, teniendo en cuenta la entidad del riesgo producido o del perjuicio causado, o el hecho de que se hubiesen producido con violencia o amenazas colectivas.

2. Infracciones graves: la realización de los actos que tengan prohibidos o la omisión de los que les corresponda realizar, dando lugar a que las medidas de seguridad obligatorias no funcionen o lo hagan defectuosamente.

3. Infracciones leves: las definidas en el apartado 1.3.º del presente artículo, bajo los párrafos c) y d).

CAPITULO II

Procedimiento

Artículo 156. *Disposición general.*

Al procedimiento sancionador le será de aplicación lo dispuesto con carácter general en el Reglamento de Procedimiento para el ejercicio de la potestad sancionadora, aprobado por Real Decreto 1398/1993, de 4 de agosto, con las especialidades previstas en los artículos siguientes.

Artículo 157. *Iniciación.*

Tienen competencia para ordenar la incoación del procedimiento sancionador y para adoptar, si procede, las medidas cautelares que determina el artículo 35 de la Ley de Seguridad Privada:

a) El Ministro de Justicia e Interior, el Secretario de Estado de Interior, el Director general de la Policía y los Gobernadores Civiles, con carácter general, y el Director general de la Guardia Civil respecto a las infracciones cometidas por guardas particulares del campo en sus distintas modalidades.

b) Para las infracciones leves:

1.º Las Jefaturas Superiores o Comisarías Provinciales de Policía.

2.º Las Comandancias de la Guardia Civil respecto a las cometidas por los guardas particulares del campo en sus distintas modalidades.

c) Todos los órganos mencionados, en materias relacionadas con medidas de seguridad, según el ámbito geográfico en que hubieran sido cometidas.

Artículo 158. *Organos instructores.*

1. La instrucción de los procedimientos sancionadores por faltas muy graves y graves corresponderá a los Gobiernos Civiles, salvo cuando corresponda a los Gobernadores Civiles el ejercicio de la potestad sancionadora.

2. La instrucción de los procedimientos sancionadores, en los supuestos no comprendidos en el apartado anterior, corresponderá a las Comisarías Provinciales de Policía y, en su caso, a las Comandancias de la Guardia Civil.

Artículo 159. *Informe.*

En los procedimientos por faltas muy graves o graves, antes de formular la propuesta de resolución, el órgano instructor, en su caso, remitirá copia del expediente instruido, e interesará informe a la unidad orgánica central de seguridad privada de la Dirección General de la Policía, que habrá de emitirlo en un plazo de quince días.

Artículo 160. *Fraccionamiento del pago.*

1. Cuando la sanción sea de naturaleza pecuniaria, la autoridad que la impuso podrá acordar, previa solicitud fundada del interesado, el fraccionamiento del pago, dentro del plazo de treinta días previsto legalmente.

2. Si se acordase el fraccionamiento del pago, éste se efectuará mediante el abono de la sanción en dos plazos, por un importe de un 50 por 100 de la misma en cada uno de ellos.

Artículo 161. *Publicación de sanciones.*

Cuando la especial transcendencia o gravedad de los hechos, el número de personas afectadas o la conveniencia de su conocimiento por los ciudadanos lo hagan aconsejable, las autoridades competentes podrán acordar que se haga pública la resolución adoptada en procedimientos sancionadores por infracciones graves o muy graves.

Disposición adicional primera. *Funciones de las Policías de las Comunidades Autónomas.*

Los órganos correspondientes y, en su caso, las Policías de las Comunidades Autónomas con competencias para la protección de personas y bienes y para el mantenimiento del orden público, con arreglo a lo dispuesto en sus Estatutos de Autonomía y lo previsto en la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad, ejercerán las facultades de autorización, inspección y sanción de las empresas de seguridad que tengan su domicilio legal en el territorio de cada Comunidad Autónoma y el ámbito de actuación limitado al mismo. También les corresponderá la denuncia, y puesta en conocimiento de las autoridades competentes, de las infracciones cometidas por las empresas de seguridad que no tengan su domicilio legal en el territorio de la Comunidad Autónoma o su ámbito de aplicación limitado al mismo. Asimismo, ejercerán las facultades en materia de seguridad privada derivadas de la disposición adicional de la Ley Orgánica 1/1992, de 21 de febrero, sobre protección de la seguridad ciudadana. En particular, les corresponden las funciones reguladas en los artículos de este Reglamento que seguidamente se determinan:

1.ª Artículo 2.1. El requisito de inscripción debe cumplimentarse en el Registro de la Comunidad Autónoma competente.

2.ª Artículo 5.1. Instrucción y resolución de las distintas fases del procedimiento de habilitación de empresas de seguridad. Conocimiento del propósito de terminación del contrato de seguro de responsabilidad civil.

3.ª Artículo 5.3. Inspección y control en materia de seguridad privada, así como requerimiento de informes sobre las características de los armeros de empresas de seguridad.

4.ª Artículo 7.1 La referencia a la Caja General de Depósitos se entenderá hecha a la caja que determine la comunidad autónoma correspondiente.

5.ª Artículo 12.2. Cancelación de inscripciones de empresas de seguridad.

6.ª Artículos 14.1 y 15. Recepción de informaciones relativas a actividades y al personal de las empresas de seguridad. Y control de comienzo de las actividades de las empresas de seguridad inscritas y autorizadas por la Comunidad Autónoma.

7.ª Artículo 17.1 y 2. Solicitud o conocimiento de la apertura de delegaciones o sucursales de empresas de seguridad.

8.ª Artículos 19.1.a), 20 y 21. Control de prestación de servicios y de los contratos correspondientes.

9.ª Artículo 24. Determinación de servicios en los que las empresas deberán garantizar la comunicación entre sus sedes y el personal que los desempeñe.

10.ª Artículo 27, apartados 3 y 4, y artículo 28 ; artículo 29, y artículo 30, apartados 1, 4 y 5.

11.ª Autorización de actividades de protección de personas, cuando se desarrollen en el ámbito territorial de la Comunidad Autónoma.

12.ª Autorizaciones provisionales de carácter inmediato para la prestación de servicios de protección personal.

13.ª Comunicación de la composición de la escolta, de sus variaciones y de la finalización del servicio, así como comunicación a las Policías de las Comunidades Autónomas de las autorizaciones concedidas, de los datos de las personas protegidas y de los escoltas y del momento de iniciación y finalización del servicio.

Los órganos correspondientes de la Comunidad Autónoma competente darán cuenta oportunamente a la Dirección General de la Policía de las autorizaciones concedidas y de las comunicaciones recibidas, de acuerdo con lo dispuesto en los mencionados artículos 27, 28, 29 y 30.

14.ª Artículo 32.1. Determinación de protección de vehículos no blindados.

15.ª Artículo 36. Supervisión de los transportes de fondos, valores u objetos.

16.ª Artículo 44. Conocimiento de las características del servicio técnico de averías.

17.ª Artículo 50. Requerimiento de subsanación de deficiencias y orden de desconexión del sistema con la central de alarmas.

18.ª Artículo 66.3. Regulación y concesión de distinciones honoríficas.

19.ª Artículo 80.2. Autorización de servicios de seguridad en polígonos industriales o urbanizaciones aisladas.

20.ª Artículo 93.3. Autorización de servicios con armas por guardas particulares del campo cuyas actividades se desarrollen en el ámbito territorial de la Comunidad Autónoma.

21.ª Artículo 96.b) y c). Disposición sobre prestación de servicios bajo la dirección de un jefe de seguridad.

22.ª Artículo 100. Comunicación de altas y bajas de los jefes de seguridad y de los directores de seguridad.

23.ª Artículos 104, 105 y 107. La apertura de despachos de detectives privados y de sus delegaciones y sucursales, así como los actos constitutivos de sociedades de detectives y sus modificaciones, en el territorio de la Comunidad Autónoma deberán ser comunicadas a ésta por la Dirección General de la Policía, tan pronto como figuren regularizados en el correspondiente Registro.

24.ª Artículo 111. Resolución sobre adopción de medidas de seguridad por parte de empresas o entidades industriales, comerciales o de servicios.

25.ª Artículo 112.1. Exigencia a las empresas o entidades para que adopten servicios o sistemas de seguridad.

26.ª Artículo 115. Comunicaciones relativas a la creación de departamentos de seguridad y a la designación de directores de seguridad.

Artículo 115. Solicitudes de creación de departamentos de seguridad.

27.ª Artículo 118. Concesión de dispensas de la implantación o mantenimiento del servicio de vigilantes de seguridad, e inspección por parte de la Policía de la Comunidad Autónoma correspondiente.

28.ª Artículo 120.2, párrafo tercero.

Autorización para la sustitución de medidas de seguridad por la implantación del servicio de vigilantes de seguridad.

29.ª Artículo 124.3. Autorización para el funcionamiento de oficinas de cambio de divisas, bancos móviles y módulos transportables.

30.ª Artículo 125. Concesión de exenciones de implantación de medidas de seguridad.

31.ª Artículo 128. Conocimiento de realización de exhibiciones o subastas de objetos de joyería o platería, así como de antigüedades u obras de arte, así como la imposición de medidas de seguridad.

32.ª Artículo 129. Dispensa de la adopción de medidas de seguridad.

33.ª Artículo 130.5 y 6. Imposición de la obligación de adoptar servicios o sistemas de seguridad a las estaciones de servicio y unidades de suministro de combustibles y carburantes, así como la dispensa de la adopción de medidas de seguridad.

34.ª Artículo 132.4. Adopción de sistemas de seguridad por parte de Administraciones de Lotería y Despachos de Apuestas Mutuas.

35.ª Artículo 136. Comprobaciones, inspecciones y autorizaciones de apertura y traslado de establecimientos u oficinas obligados a disponer de medidas de seguridad, y de instalación, modificación y traslado de cajeros automáticos.

36.ª Artículo 137.1. Competencia de control en materia de seguridad privada.

37.ª Artículo 137.2. Colaboración de la Policía para el ejercicio de la función de control.

38.ª Artículo 137.3. Control de las actuaciones de los guardas particulares del campo.

39.ª Artículo 138. Del informe anual de actividades de las empresas de seguridad que tengan su domicilio social y su ámbito de actuación limitado al territorio de una Comunidad Autónoma competente en la materia, que sea remitido a la Secretaría de Estado de Interior, será enviada copia por dicha Secretaría al órgano correspondiente de la Comunidad Autónoma.

40.ª Artículo 140. Comunicación de modificaciones de empresas de seguridad inscritas en el Registro de la Comunidad Autónoma.

41.ª Artículo 141. De la memoria anual de actividades de los detectives privados con despachos, delegaciones o sucursales sitos exclusivamente en el territorio de una Comunidad Autónoma competente en la materia, que sea remitida a la Secretaría de Estado de Interior, será enviada copia por dicha Secretaría al órgano correspondiente de la Comunidad Autónoma.

42.ª Artículo 143. Disposición de los libros-registro de las empresas de seguridad, y de los detectives privados, y acceso a armeros, cámaras acorazadas e instalaciones de aquéllas ; todo ello a efectos de inspección y control.

43.ª Artículo 145. Adopción de la medida cautelar de ocupación o precinto y ratificación de la misma, en su caso.

44.ª Artículo 147. Suspensión y ratificación de la suspensión, de servicios de seguridad privada o de la utilización de medios materiales o técnicos.

45.ª Artículo 157.2. Competencia para ordenar la incoación de procedimientos sancionadores y para adoptar medidas cautelares en relación con las empresas de seguridad.

46.ª Artículo 158. Competencia para la instrucción de procedimientos sancionadores a las empresas de seguridad.

47.ª Artículos 160 y 162. Competencia para la emisión de informe y para acordar la publicación de la sanción.

Disposición adicional segunda. *Reducción de los mínimos de garantía.*

Las cantidades determinantes de los mínimos de garantía, especificadas en el apartado I del anexo a este Reglamento, cualesquiera que fueren las actividades que realicen o servicios que presten, quedarán reducidas al 50 por 100, cuando se trate de empresas que tengan una plantilla de menos de 50 trabajadores, y durante dos años consecutivos no superen los 601.012,10 euros (100.000.000 de pesetas) de facturación anual.

Disposición derogatoria única.

Queda derogado el apartado 2 del artículo 30 y el apartado 5 del artículo 43 del Reglamento de Seguridad Privada.

Disposición final primera. *Efectos de la falta de resoluciones expresas.*

Las solicitudes de autorizaciones, dispensas y exenciones, así como las de habilitaciones de personal, reguladas en el presente Reglamento se podrán considerar desestimadas y se podrán interponer contra su desestimación los recursos procedentes, si no recaen sobre ellas resoluciones expresas dentro del plazo de tres meses y de la ampliación del mismo, en su caso, salvo que tengan plazos específicos establecidos en el presente Reglamento, a partir de la fecha en que la solicitud haya tenido entrada en cualquiera de los registros del órgano administrativo competente, sin perjuicio de la obligación de las autoridades competentes de resolver expresamente.

Disposición final segunda. *Uso o consumo de productos provenientes de Estados miembros de la Unión Europea.*

Las normas contenidas en el presente Reglamento y en los actos y disposiciones de desarrollo y ejecución del mismo, sobre vehículos y material de seguridad, no impedirán el uso o consumo en España de productos provenientes de otros Estados miembros de la Unión Europea, que respondan, en lo concerniente a la seguridad, a normas equivalentes a las del Estado español, y siempre que ello se haya establecido mediante la realización de ensayos o pruebas de conformidad equivalentes a las exigidas en España.

ANEXO

Requisitos específicos de las empresas de seguridad, según las distintas clases de actividad

I. Requisitos de inscripción y autorización inicial.

1. Vigilancia y protección de bienes, establecimientos, certámenes o convenciones.

A) Fase inicial.

Si se trata de sociedades, acreditar que cumple los requisitos previstos en el artículo 5.1.a),1.º

B) Segunda fase.

Relación del personal disponible en la que constará necesariamente el jefe de seguridad y los vigilantes de seguridad.

C) Tercera fase.

a) Tener instalado en los locales de la empresa, tanto en el principal como en los de las delegaciones o sucursales, armero o caja fuerte de las características que determine el Ministerio del Interior.

b) Tener concertado contrato de seguro de responsabilidad civil, aval u otra garantía financiera con entidad debidamente autorizada con una cuantía mínima de 300.506,10 euros por siniestro y año.

c) Tener constituida, en la forma que se determina en el artículo 7 de este reglamento, una garantía de 240.404,84 euros si el ámbito de actuación es estatal y de 48.080,97 euros, más 12.020,24 euros por provincia, si el ámbito de actuación es autonómico.

2. Protección de personas.

A) Fase inicial.

Si se trata de sociedades, acreditar que cumple los requisitos previstos en el artículo 5.1.a),1.º

B) Segunda fase.

Relación del personal disponible en la que constará necesariamente el jefe de seguridad y los escoltas privados.

C) Tercera fase.

a) Tener instalado en los locales de la empresa, tanto en el principal como en los de las delegaciones o sucursales, un armero o caja fuerte de las características que determine el Ministerio del Interior.

b) Tener concertado un seguro de responsabilidad civil, aval u otra garantía financiera, con entidad debidamente autorizada con una cuantía mínima de 601.012,10 euros por siniestro y año.

c) Tener constituida, en la forma determinada en el artículo 7 de este reglamento, una garantía de 240.404,84 euros.

d) Disponer de medios de comunicación suficientes para garantizar la comunicación entre las unidades periféricas móviles y la estación base.

3. Depósito, custodia y tratamiento de objetos valiosos o peligrosos, y custodia de explosivos.

3.1 Objetos valiosos o peligrosos.

A) Fase inicial. Si se trata de sociedades, acreditar que cumple los requisitos previstos en el artículo 5.1.a),1.º

B) Segunda fase.

Relación del personal disponible en la que constará necesariamente el jefe de seguridad y los vigilantes que integran el servicio de seguridad.

C) Tercera fase.

a) Tener concertado contrato de seguro de responsabilidad civil, aval u otra garantía financiera con entidad debidamente autorizada con una cuantía mínima de 601.012,42 euros por siniestro y año.

b) Tener constituida una garantía de 240.404,84 euros si se trata de empresa de ámbito estatal, y de 60.101,21 euros, más 12.020,4 euros por provincia, si es empresa de ámbito autonómico.

c) Tener instalado en los locales de la empresa, tanto en el principal como en los de las delegaciones o sucursales, armero o caja fuerte de las características determinadas por el Ministerio del Interior.

d) Tener instalada cámara acorazada y locales anejos de las características y con el sistema de seguridad que determine el Ministerio del Interior.

Los requisitos relativos a cámara acorazada, vigilantes de seguridad que integran el servicio de seguridad y armero o caja fuerte, se exigirán por cada inmueble que destine la empresa a esta actividad.

3.2 Explosivos.

A) Fase inicial.
Si se trata de sociedades, acreditar que cumple los requisitos previstos en el artículo 5.1.a),1.º
B) Segunda fase.
Servicio de seguridad compuesto por un jefe de seguridad y una dotación de, al menos, cinco vigilantes de explosivos, por cada depósito comercial o de consumo de explosivos en el que se preste servicio de custodia.
C) Tercera fase.

a) Tener concertado contrato de seguro de responsabilidad civil, aval u otra garantía financiera con entidad debidamente autorizada con una cuantía mínima de 601.012,10 euros por siniestro y año.
b) Tener constituida una garantía de 120.202,42 euros, si se trata de empresa de ámbito estatal, y de 30.050,61 euros, más 6.010,12 euros por provincia, si la empresa es de ámbito autonómico.
c) Depósito de almacenamiento y armero o caja fuerte, de las características y con el sistema de seguridad, en su caso, que determine el Ministerio del Interior.

4. Transporte y distribución de objetos valiosos o peligrosos y de explosivos.

4.1 Objetos valiosos o peligrosos.

A) Fase inicial.
Si se trata de sociedades, acreditar que cumple los requisitos previstos en el artículo 5.1.a), 1.º
B) Segunda fase.

a) Relación del personal disponible en la que constará necesariamente el jefe de seguridad y los vigilantes de seguridad.
b) Seis vehículos blindados, si la empresa es de ámbito estatal y dos, si la empresa es de ámbito autonómico. Los vehículos tendrán las características que determine el Ministerio del Interior, estarán dotados de permiso de circulación, tarjeta de industrial y certificado acreditativo de la superación de la inspección técnica, todo ello a nombre de la empresa solicitante.
c) Local destinado exclusivamente a la guarda de los vehículos blindados fuera de las horas de servicio.

C) Tercera fase.

a) Tener concertado contrato de seguro de responsabilidad civil, aval u otra garantía financiera con entidad debidamente autorizada con una cuantía mínima de 601.012,10 euros por siniestro y año.
b) Una garantía de 240.404,84 euros, si la empresa es de ámbito estatal, y de 48.080,97 euros, más 12.020,24 euros por provincia, si es de ámbito autonómico.
c) Tener instalado en los locales de la empresa, tanto en el principal como en los de las delegaciones o sucursales, armero o caja fuerte de las características que determine el Ministerio del Interior.
d) Disponer de un servicio de telecomunicación de voz entre los locales de la empresa, tanto el principal como los de las sucursales o delegaciones, y los vehículos que realicen el transporte.

4.2 Explosivos.

A) Fase inicial.
Si se trata de sociedades, acreditar que cumple los requisitos previstos en el artículo 5.1.a),1.º
B) Segunda fase.

a) Una plantilla compuesta por, al menos, dos vigilantes de explosivos por cada vehículo para el transporte de explosivos de que disponga la empresa y un jefe de seguridad cuando el número de vigilantes exceda de quince en total.

b) Disponer para el transporte de explosivos, al menos, de dos vehículos blindados con capacidad de carga superior a 1.000 kg cada uno, con las características que determina el Reglamento Nacional del Transporte de Mercancías Peligrosas por Carretera (TPC, tipo 2), y con las medidas de seguridad que se establezcan, debiendo aportar los documentos que para su acreditación determine el Ministerio del Interior.

c) Local para la guarda de los vehículos durante las horas en que permanecieren inmovilizados.

C) Tercera fase.

a) Tener concertado contrato de seguro de responsabilidad civil, aval u otra garantía financiera con entidad debidamente autorizada con una cuantía mínima de 601.012,42 euros por siniestro y año.

b) Una garantía de 120.202,42 euros, si la empresa es de ámbito estatal, y de 30.050,61 euros, más 6.010,12 euros por provincia, si es de ámbito autonómico.

c) Tener instalado armero o caja fuerte de las características que determine el Ministerio del Interior.

d) Disponer de un servicio de telecomunicación de voz entre los locales de la empresa, tanto el principal como los de las sucursales o delegaciones, y los vehículos que realicen el transporte.

5. Instalación y mantenimiento de aparatos, dispositivos y sistemas de seguridad.

A) Fase inicial.

Si se trata de sociedades, acreditar que cumple los requisitos previstos en el artículo 5.1.a), 1.º

B) Segunda fase.

a) Relación de personal disponible en la que constará necesariamente el ingeniero técnico y los instaladores.

b) Una zona o área restringida que, con medios físicos, electrónicos o informáticos, garantice la custodia de la información que manejaren y de la que serán responsables.

C) Tercera fase.

a) Tener constituida una garantía de 120.202,42 euros, para el ámbito estatal, y de 30.050,61 euros, más 6.010,12 euros por provincia, para el ámbito autonómico.

b) Tener concertado contrato de seguro de responsabilidad civil, aval u otra garantía financiera con entidad debidamente autorizada con una cuantía mínima de 300.506,05 euros por siniestro y año.

6. Explotación de centrales de alarma.

A) Fase inicial

Si se trata de sociedades, acreditar que cumple los requisitos previstos en el artículo 5.1.a),1.º

B) Segunda fase.

a) Elementos, equipos o sistemas capacitados para la recepción y verificación de las señales de alarma y su transmisión a las Fuerzas y Cuerpos de Seguridad.

b) Locales cuyos requisitos y características del sistema de seguridad determine el Ministerio del Interior.

c) Un sistema de alimentación ininterrumpida de energía que garantice durante veinticuatro horas, al menos, el funcionamiento de la central en el caso de corte del suministro de fluido eléctrico.

C) Tercera fase.

a) Tener constituida una garantía de 120.202,42 euros.

b) Tener concertado contrato de seguro de responsabilidad civil, aval u otra garantía financiera con entidad debidamente autorizada con una cuantía mínima de 300.506,05 euros.

7. Planificación y asesoramiento de actividades de seguridad.

A) Segunda fase.

a) Relación del personal disponible en la que constará necesariamente personal facultativo con la competencia suficiente para responsabilizarse de los proyectos, en los casos en que su actividad tenga por objeto el diseño de proyectos de instalaciones y sistemas de seguridad.

b) Si se trata de sociedades, acreditar que cumple los requisitos previstos en el artículo 5.1.a),1.º

c) Un área o zona restringida que, con medios físicos, electrónicos o informáticos, garantice la custodia de la información que manejare la empresa y de la que será responsable.

d) Cuando el asesoramiento o la planificación tengan por objeto alguna de las actividades a que se refieren los párrafos a), b), c) y d) del artículo 5 de la Ley 23/1992, de 30 de julio, de Seguridad Privada, disponer, en la plantilla, de personal que acredite, mediante la justificación del desempeño de puestos o funciones de seguridad pública o privada, al menos, durante cinco años, conocimientos y experiencia sobre organización y realización de actividades de seguridad.

B) Tercera fase.

a) Tener constituida una garantía por importe de 60.101,21 euros.

b) Tener concertado contrato de seguro de responsabilidad civil, aval u otra garantía financiera con entidad debidamente autorizada con una cuantía mínima de 300.506,05 euros por siniestro y año.

8. Requisitos de las empresas que tengan su domicilio en Ceuta y Melilla.

Las empresas de seguridad con domicilio social en Ceuta y en Melilla, que pretendan desarrollar su actividad únicamente en el ámbito de una de dichas ciudades, deberán cumplir los mismos requisitos establecidos en el presente anexo.

II. Requisitos de las empresas de ámbito autonómico.

1. Las cantidades determinantes de los mínimos de garantía y de seguro de responsabilidad civil, aval u otra garantía financiera con entidad debidamente autorizada, especificadas en el apartado I de este anexo, como requisitos "De inscripción y autorización inicial", relativos a las empresas de ámbito autonómico, sean cuales fueren las actividades que realicen o servicios que presten, quedarán reducidas al 75 por ciento o al 50 por ciento, según que la población de derecho de las correspondientes comunidades autónomas sea inferior a 2.000.000 de habitantes y superior a 1.250.000, o inferior a 1.250.000 habitantes.

2. Las cantidades determinantes de los mínimos de garantía, especificadas en el apartado I de este anexo, relativas a las empresa de seguridad de ámbito autonómico, cualesquiera que fueren las actividades que realicen o servicios que presten, y cualquiera que fuere la población de derecho de las correspondientes comunidades autónomas, quedarán reducidas al 50 por ciento cuando se trate de empresas que, en el momento de la inscripción en el Registro, tengan una plantilla de menos de 50 trabajadores, y asimismo cuando, posteriormente, durante dos años consecutivos, no superen los 601.012,10 euros de facturación anual.

La reducción establecida en este apartado 2 no será acumulable a la relativa al mínimo de garantía, comprendida en lo dispuesto en el apartado anterior.

3. En los supuestos contemplados en los apartados 1 y 2 precedentes, no se computarán las cantidades por provincia, especificadas en el apartado I de este anexo, en cuanto a garantía, respecto a las provincias que tengan menos de 250.000 habitantes de población de derecho.

4. Respecto a las empresas de seguridad de ámbito autonómico, dedicadas exclusivamente a instalación y mantenimiento de aparatos, dispositivos y sistemas de seguridad, los requisitos establecidos en el apartado I.5 de este anexo, se aplicarán con las modificaciones que se especifican a continuación:

a) No necesitarán tener un ingeniero técnico en la plantilla a tiempo total, cuando ésta integre menos de cinco puestos de instaladores, si bien, alternativamente, habrán de tenerlo a tiempo parcial, o deberán contar, de forma permanente, mediante contrato mercantil, con

los servicios de un ingeniero técnico que supervise y garantice técnicamente la instalación y el mantenimiento de aparatos, dispositivos y sistemas. En todo caso, el ingeniero técnico habrá de estar específicamente cualificado par el ejercicio de su misión.

b) La garantía mínima a constituir será de 6.101,21 euros.

Sin embargo, será de 12.020,24 euros, cuando se trate de empresas no constituidas en forma de sociedad.

c) El contrato de seguro de responsabilidad civil, aval u otra garantía financiera con entidad debidamente autorizada cubrirá una garantía mínima de 60.101,21 euros.

5. Las modificaciones de plantillas de las empresas autonómicas a que se refiere el presente apartado, que den lugar a su inclusión o exclusión del supuesto regulado en el apartado 2 anterior, producirán el cambio de los requisitos de inscripción y autorización de dichas empresas y determinarán la instrucción de los correspondientes expedientes de modificaciones de inscripción.

6. Cuando las empresas pretendan actuar en comunidades autónomas limítrofes, sin abarcar la totalidad del territorio nacional, deberán inscribirse en el Registro General de Empresas de Seguridad, pero podrán hacerlo con aplicación de los criterios cuantitativos, establecidos en este anexo, conjuntamente a los ámbitos territoriales autonómicos correspondientes, como si se tratara de un territorio autonómico único.

§ 29

Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 166, de 12 de julio de 2002
Última modificación: 23 de enero de 2025
Referencia: BOE-A-2002-13758

[. . .]

Disposición adicional novena. *Gestión de incidentes de ciberseguridad que afecten a la red de Internet.*

1. Los prestadores de servicios de la Sociedad de la Información, los registros de nombres de dominio y los agentes registradores que estén establecidos en España están obligados a prestar su colaboración con el CERT competente, en la resolución de incidentes de ciberseguridad que afecten a la red de Internet y actuar bajo las recomendaciones de seguridad indicadas o que sean establecidas en los códigos de conducta que de esta Ley se deriven.

Los órganos, organismos públicos o cualquier otra entidad del sector público que gestionen equipos de respuesta a incidentes de seguridad colaborarán con las autoridades competentes para la aportación de las evidencias técnicas necesarias para la persecución de los delitos derivados de dichos incidentes de ciberseguridad.

2. Para el ejercicio de las funciones y obligaciones anteriores, los prestadores de servicios de la Sociedad de la información, respetando el secreto de las comunicaciones, suministrarán la información necesaria al CERT competente, y a las autoridades competentes, para la adecuada gestión de los incidentes de ciberseguridad, incluyendo las direcciones IP que puedan hallarse comprometidas o implicadas en los mismos.

De la misma forma, los órganos, organismos públicos o cualquier otra entidad del sector público que gestionen equipos de respuesta a incidentes de seguridad podrán intercambiar información asociada a incidentes de ciberseguridad con otros CERTs o autoridades competentes a nivel nacional e internacional, siempre que dicha información sea necesaria para la prevención de incidentes en su ámbito de actuación.

3. El Gobierno pondrá en marcha, en el plazo de seis meses, un programa para impulsar un esquema de cooperación público-privada con el fin de identificar y mitigar los ataques e incidentes de ciberseguridad que afecten a la red de Internet en España. Para ello, se elaborarán códigos de conducta en materia de ciberseguridad aplicables a los diferentes prestadores de servicios de la sociedad de la información, y a los registros de nombres de dominio y agentes registradores establecidos en España.

Los códigos de conducta determinarán el conjunto de normas, medidas y recomendaciones a implementar que permitan garantizar una gestión eficiente y eficaz de dichos incidentes de ciberseguridad, el régimen de colaboración y condiciones de adhesión e implementación, así como los procedimientos de análisis y revisión de las iniciativas resultantes.

La Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información coordinará las actuaciones que se pongan en marcha derivadas de estos códigos de conducta.

4. Conforme a los códigos de conducta que se definan en particular, los prestadores de servicios de la sociedad de la información deberán identificar a los usuarios afectados por los incidentes de ciberseguridad que les sean notificados por el CERT competente, e indicarles las acciones que deben llevar a cabo y que están bajo su responsabilidad, así como los tiempos de actuación. En todo caso, se les proporcionará información sobre los perjuicios que podrían sufrir u ocasionar a terceros si no colaboran en la resolución de los incidentes de ciberseguridad a que se refiere esta disposición.

En el caso de que los usuarios no ejerciesen en el plazo recomendado su responsabilidad en cuanto a la desinfección o eliminación de los elementos causantes del incidente de ciberseguridad, los prestadores de servicios deberán, bajo requerimiento del CERT competente, aislar dicho equipo o servicio de la red, evitando así efectos negativos a terceros hasta el cese de la actividad maliciosa.

El párrafo anterior será de aplicación a cualquier equipo o servicio geolocalizado en España o que esté operativo bajo un nombre de dominio «.es» u otros cuyo Registro esté establecido en España.

5. Reglamentariamente se determinará los órganos, organismos públicos o cualquier otra entidad del sector público que ejercerán las funciones de equipo de respuesta a incidentes de seguridad o CERT competente a los efectos de lo previsto en la presente disposición.

6. La Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información garantizará un intercambio fluido de información con la Secretaría de Estado de Seguridad del Ministerio del Interior sobre incidentes, amenazas y vulnerabilidades según lo contemplado en la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la Protección de las Infraestructuras Críticas. En este sentido se establecerán mecanismos de coordinación entre ambos órganos para garantizar la provisión de una respuesta coordinada frente a incidentes en el marco de la presente Ley.

[. . .]

§ 30

Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional

Ministerio de Defensa
«BOE» núm. 68, de 19 de marzo de 2004
Última modificación: sin modificaciones
Referencia: BOE-A-2004-5051

La sociedad española demanda unos servicios de inteligencia eficaces, especializados y modernos, capaces de afrontar los nuevos retos del actual escenario nacional e internacional.

Entre los elementos más característicos de esta nueva situación figuran el desarrollo alcanzado por las tecnologías de la información, la facilidad y flexibilidad de su transmisión en diversos soportes, la generalización casi universal de su uso y la accesibilidad global a las diversas herramientas y redes. Todos estos rasgos facilitan el intercambio ágil y flexible de información en las sociedades modernas.

Al mismo tiempo, la elaboración, conservación y utilización de determinada información por parte de la Administración es necesaria para garantizar su funcionamiento eficaz al servicio de los intereses nacionales.

En consecuencia, la Administración debe dotarse de los medios adecuados para la protección y control del acceso a dicha información, y ha de regular unos procedimientos eficaces para su almacenamiento, procesamiento y transmisión seguros por medio de sistemas propios.

Razones de eficacia, economía y coherencia administrativa recomiendan el establecimiento de medidas para regular y coordinar la adquisición del sofisticado material que se precisa, la homologación de su capacidad y compatibilidad, sus procedimientos de empleo y la formación técnica del personal de la Administración especialista en este campo. Asimismo, ha de elaborarse y mantenerse actualizada la normativa relativa a la protección de la información clasificada y velar por su cumplimiento, para evitar el acceso a ésta de individuos, grupos y Estados no autorizados.

El concepto de seguridad de los sistemas de información no sólo abarca la protección de la confidencialidad de ésta; en la mayoría de los casos es necesario también que los sistemas permitan el acceso de los usuarios autorizados, funcionen de manera íntegra y garanticen que la información que manejan mantiene su integridad. En consecuencia, la seguridad de los sistemas de información debe garantizar la confidencialidad, la disponibilidad y la integridad de la información que manejan y la disponibilidad y la integridad de los propios sistemas.

Se hace necesaria la participación de un organismo que, partiendo de un conocimiento de las tecnologías de la información y de las amenazas y vulnerabilidades que existen, proporcione una garantía razonable sobre la seguridad de productos y sistemas. A partir de

esa garantía, los responsables de los sistemas de información podrán implementar los productos y sistemas que satisfagan los requisitos de seguridad de la información.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional en su artículo 9.2.f).

Este real decreto se dicta en virtud de lo dispuesto en la disposición final primera de la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia.

En su virtud, a propuesta del Ministro de Defensa, con la aprobación previa de la Ministra de Administraciones Públicas, de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros en su reunión del día 12 de marzo de 2004,

DISPONGO:

Artículo 1. *Del Director del Centro Criptológico Nacional.*

El Secretario de Estado Director del Centro Nacional de Inteligencia, como Director del Centro Criptológico Nacional (CCN), es la autoridad responsable de coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, garantizar la seguridad de las tecnologías de la información en ese ámbito, informar sobre la adquisición coordinada del material criptológico y formar al personal de la Administración especialista en este campo. En este sentido, el Director del CCN es la autoridad de certificación de la seguridad de las tecnologías de la información y autoridad de certificación criptológica.

Asimismo es responsable de velar por el cumplimiento de la normativa relativa a la protección de la información clasificada en los aspectos de los sistemas de información y telecomunicaciones, de acuerdo a lo señalado en el artículo 4.e) y f) de la Ley 11/2002, de 6 de mayo.

Artículo 2. *Del ámbito de actuación y funciones del Centro Criptológico Nacional.*

1. El ámbito de actuación del Centro Criptológico Nacional comprende:

a) La seguridad de los sistemas de las tecnologías de la información de la Administración que procesan, almacenan o transmiten información en formato electrónico, que normativamente requieren protección, y que incluyen medios de cifra.

b) La seguridad de los sistemas de las tecnologías de la información que procesan, almacenan o transmiten información clasificada.

2. Dentro de dicho ámbito de actuación, el Centro Criptológico Nacional realizará las siguientes funciones:

a) Elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración. Las acciones derivadas del desarrollo de esta función serán proporcionales a los riesgos a los que esté sometida la información procesada, almacenada o transmitida por los sistemas.

b) Formar al personal de la Administración especialista en el campo de la seguridad de los sistemas de las tecnologías de la información y las comunicaciones.

c) Constituir el organismo de certificación del Esquema nacional de evaluación y certificación de la seguridad de las tecnologías de información, de aplicación a productos y sistemas en su ámbito.

d) Valorar y acreditar la capacidad de los productos de cifra y de los sistemas de las tecnologías de la información, que incluyan medios de cifra, para procesar, almacenar o transmitir información de forma segura.

e) Coordinar la promoción, el desarrollo, la obtención, la adquisición y puesta en explotación y la utilización de la tecnología de seguridad de los sistemas antes mencionados.

f) Velar por el cumplimiento de la normativa relativa a la protección de la información clasificada en su ámbito de competencia.

g) Establecer las necesarias relaciones y firmar los acuerdos pertinentes con organizaciones similares de otros países, para el desarrollo de las funciones mencionadas.

Para el desarrollo de estas funciones, el CCN podrá establecer la coordinación oportuna con las comisiones nacionales a las que las leyes atribuyan responsabilidades en el ámbito de los sistemas de las tecnologías de la información y de las comunicaciones.

3. El Centro Criptológico Nacional queda adscrito al Centro Nacional de Inteligencia y comparte con éste medios, procedimientos, normativa y recursos, y se regirá por la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia. El personal del CCN estará integrado orgánica y funcionalmente en el Centro Nacional de Inteligencia, por lo que le serán de aplicación todas las disposiciones relativas al personal de éste, contempladas en la Ley 11/2002, de 6 de mayo, y en la normativa de desarrollo, particularmente su régimen estatutario.

Disposición derogatoria única. *Derogación normativa.*

Quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en este real decreto.

Disposición final primera. *Facultades de desarrollo.*

Se faculta al Ministro de Defensa para dictar cuantas disposiciones sean necesarias para la aplicación y el desarrollo de lo establecido en este real decreto.

Disposición final segunda. *Entrada en vigor.*

El presente real decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

§ 31

Real Decreto 521/2020, de 19 de mayo, por el que se establece la organización básica de las Fuerzas Armadas. [Inclusión parcial]

Ministerio de Defensa
«BOE» núm. 143, de 21 de mayo de 2020
Última modificación: sin modificaciones
Referencia: BOE-A-2020-5190

[. . .]

TÍTULO II

Estructura operativa de las Fuerzas Armadas

[. . .]

CAPÍTULO II

El Estado Mayor de la Defensa

Funciones y estructura del Estado Mayor de la Defensa

Artículo 9. *El Estado Mayor de la Defensa.*

1. El Estado Mayor de la Defensa es el órgano que posibilita el cumplimiento de sus funciones al Jefe de Estado Mayor de la Defensa. Se organizará de forma que permita la definición y el desarrollo de la estrategia militar, el planeamiento militar, el planeamiento, seguimiento y conducción de las operaciones militares, asegurar la eficacia operativa de las Fuerzas Armadas y su transformación y avance digital y el ejercicio del resto de sus competencias.

2. Entre otras funciones, al Estado Mayor de la Defensa le corresponderá:

a) El desarrollo y detalle de las políticas de Seguridad de la Información en los Sistemas de Información y Telecomunicaciones en el marco de las políticas establecidas, así como la dirección de la ejecución y el control del cumplimiento de estas políticas en el ámbito de las Fuerzas Armadas y para las operaciones.

b) Apoyar al Jefe de Estado Mayor de la Defensa en las actuaciones que deba realizar sobre la Infraestructura Integral de Información para la Defensa en el ámbito operativo y en las que debiera realizar para la supervivencia de los servicios de los sistemas de telecomunicaciones e información críticos para la defensa y las Fuerzas Armadas, con el alcance necesario para garantizar la operatividad del Sistema de Mando y Control Militar.

c) La planificación, dirección y, en su caso, ejecución de las actuaciones en materia de información geoespacial que le correspondan en su ámbito de competencias, sin perjuicio de

las responsabilidades asignadas a otros organismos de los Ejércitos y de la Armada, de acuerdo con la normativa en vigor.

d) La dirección y coordinación de la sanidad operativa.

3. El Estado Mayor de la Defensa se estructurará en un Cuartel General y los siguientes órganos:

a) El Mando de Operaciones.
b) El Centro de Inteligencia de las Fuerzas Armadas.
c) El Mando Conjunto del Ciberespacio.
d) El Centro Superior de Estudios de la Defensa Nacional.

4. Además, en el Estado Mayor de la Defensa se integrarán:

a) Las organizaciones operativas permanentes.
b) Los órganos nacionales militares relacionados con organizaciones internacionales o multinacionales.

[. . .]

CAPÍTULO IV

Los órganos de la estructura del Estado Mayor de la Defensa

[. . .]

Artículo 13. *El Mando Conjunto del Ciberespacio.*

1. El Mando Conjunto del Ciberespacio es el órgano responsable de la dirección, la coordinación, el control y la ejecución de las acciones conducentes a asegurar la libertad de acción de las Fuerzas Armadas en el ámbito ciberespacial.

2. Para ello, el Mando Conjunto del Ciberespacio planea, dirige, coordina, controla y ejecuta las operaciones militares en el ciberespacio y, en este ámbito, las acciones necesarias para garantizar la supervivencia de los elementos físicos, lógicos y virtuales críticos para la Defensa y las Fuerzas Armadas.

[. . .]

§ 32

Orden DEF/710/2020, de 27 de julio, por la que se desarrolla la organización básica del Estado Mayor de la Defensa. [Inclusión parcial]

Ministerio de Defensa
«BOE» núm. 204, de 28 de julio de 2020
Última modificación: 12 de octubre de 2023
Referencia: BOE-A-2020-8638

[. . .]

Disposición adicional segunda. *Atribuciones del Comandante del Mando Conjunto del Ciberespacio.*

El Comandante del Mando Conjunto del Ciberespacio asumirá, además de sus nuevas responsabilidades, las atribuciones que tenga conferidas el Comandante del Mando Conjunto de Ciberdefensa, según la normativa en vigor.

[. . .]

ORGANIZACIÓN DEL ESTADO MAYOR DE LA DEFENSA

Artículo 1. *Organización del Estado Mayor de la Defensa.*

1. El Estado Mayor de la Defensa (EMAD) se estructura de la siguiente forma:

a) El Cuartel General del Estado Mayor de la Defensa.
b) El Mando de Operaciones.
c) El Centro de Inteligencia de las Fuerzas Armadas.
d) El Mando Conjunto del Ciberespacio.
e) El Centro Superior de Estudios de la Defensa Nacional.

2. Directamente subordinados al Jefe de Estado Mayor de la Defensa (JEMAD), se encuentran:

a) Las organizaciones operativas permanentes:

1.º El Mando Operativo Terrestre.
2.º El Mando Operativo Marítimo.
3.º El Mando Operativo Aéreo.
4.º El Mando Operativo Espacial.
5.º El Mando Operativo Ciberespacial.

b) Los órganos nacionales militares relacionados con organizaciones internacionales o multinacionales.

[. . .]

Artículo 9. *El Mando Conjunto del Ciberespacio.*

1. El Mando Conjunto del Ciberespacio (MCCE) es el órgano responsable del planeamiento, la dirección, la coordinación, el control y la ejecución de las acciones conducentes a asegurar la libertad de acción de las FAS en el ámbito ciberespacial. Para cumplir su misión, planea, dirige, coordina, controla y ejecuta las operaciones militares en el ciberespacio, de acuerdo con los planes operativos en vigor. En el ámbito de estas operaciones, realiza las acciones necesarias para garantizar la supervivencia de los elementos físicos, lógicos y virtuales críticos para la Defensa y las FAS.

2. Asegura la autoridad del JEMAD sobre la Infraestructura Integral de Información para la Defensa (I3D) en el ámbito operativo. Colabora en la transformación digital del Ministerio de Defensa, en el ámbito del EMAD, en coordinación con el EMACON.

3. Es responsable, en colaboración con el EMACON, de la definición de requisitos operativos, seguimiento de la obtención y el sostenimiento de los medios de Ciberdefensa, de los Sistemas de Información y Telecomunicaciones (CIS) conjuntos de Mando y Control, de Guerra Electrónica y Navegación e Identificación, velando por la interoperabilidad de estos con los específicos de los Ejércitos y de la Armada. Asimismo, ha de prestar el apoyo CIS a la estructura del EMAD.

4. El MCCE incluye el Equipo de Respuesta ante Emergencias Informáticas del MINISDEF, con la denominación CERT de Defensa (ESPDEF-CERT).

5. El MCCE se articulará en:

a) La Comandancia.
b) La Segunda Comandancia.
c) El Estado Mayor del MCCE (EMMCCE).
d) La Fuerza de Operaciones en el Ciberespacio (FOCE).
e) La Jefatura de Mando y Control (JMC).
f) La Jefatura de Sistemas de Ciberdefensa (JSCD).
g) La Jefatura de Telecomunicaciones y Guerra Electrónica (JTEW).
h) La Jefatura de Apoyo CIS al EMAD (JEACISEMAD).
i) La Escuela Militar de Ciberoperaciones (EMCO).
j) Otras unidades que se determinen.

6. El EMMCCE es el principal órgano auxiliar del Comandante del MCCE, llevando a cabo las actividades de planeamiento, organización, coordinación, seguimiento y control del MCCE.

7. La FOCE es responsable de la ejecución de las operaciones militares que aseguren la libertad de acción de las FAS en el ciberespacio. En el ámbito de las citadas operaciones militares, dirige operativa y técnicamente las actividades de los Centros de Operaciones de Seguridad (COS) de las FAS. Coordina con los Ejércitos, la Armada y el Centro de Sistemas y Tecnologías de la Información y las Comunicaciones (CESTIC) las acciones necesarias. Cuando se estén realizando operaciones en el espectro electromagnético, coordinará que la ejecución de las acciones ciber se realiza de forma concurrente con éstas.

8. La EMCO es responsable de impartir las enseñanzas de perfeccionamiento en el ámbito de las ciberoperaciones y aquellas otras que se determinen relacionadas con la ciberdefensa. La EMCO dependerá funcionalmente del Centro Superior de Estudios de la Defensa Nacional (CESEDEN) para aquellos aspectos relacionados con la aprobación de los perfiles de ingreso y egreso, currículos y convocatorias de cursos conjuntos que formen parte de las enseñanzas de perfeccionamiento a impartir en esta Escuela.

[. . .]

§ 33

Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico

Jefatura del Estado
«BOE» núm. 166, de 12 de julio de 2002
Última modificación: 23 de enero de 2025
Referencia: BOE-A-2002-13758

JUAN CARLOS I REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente Ley.

EXPOSICIÓN DE MOTIVOS

I

La presente Ley tiene como objeto la incorporación al ordenamiento jurídico español de la Directiva 2000/31/CE, del Parlamento Europeo y del Consejo, de 8 de junio, relativa a determinados aspectos de los servicios de la sociedad de la información, en particular, el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico). Asimismo, incorpora parcialmente la Directiva 98/27/CE, del Parlamento Europeo y del Consejo, de 19 de mayo, relativa a las acciones de cesación en materia de protección de los intereses de los consumidores, al regular, de conformidad con lo establecido en ella, una acción de cesación contra las conductas que contravengan lo dispuesto en esta Ley.

Lo que la Directiva 2000/31/CE denomina "sociedad de la información" viene determinado por la extraordinaria expansión de las redes de telecomunicaciones y, en especial, de Internet como vehículo de transmisión e intercambio de todo tipo de información. Su incorporación a la vida económica y social ofrece innumerables ventajas, como la mejora de la eficiencia empresarial, el incremento de las posibilidades de elección de los usuarios y la aparición de nuevas fuentes de empleo.

Pero la implantación de Internet y las nuevas tecnologías tropieza con algunas incertidumbres jurídicas, que es preciso aclarar con el establecimiento de un marco jurídico adecuado, que genere en todos los actores intervinientes la confianza necesaria para el empleo de este nuevo medio.

Eso es lo que pretende esta Ley, que parte de la aplicación a las actividades realizadas por medios electrónicos de las normas tanto generales como especiales que las regulan, ocupándose tan sólo de aquellos aspectos que, ya sea por su novedad o por las peculiaridades que implica su ejercicio por vía electrónica, no están cubiertos por dicha regulación.

II

Se acoge, en la Ley, un concepto amplio de "servicios de la sociedad de la información", que engloba, además de la contratación de bienes y servicios por vía electrónica, el suministro de información por dicho medio (como el que efectúan los periódicos o revistas que pueden encontrarse en la red), las actividades de intermediación relativas a la provisión de acceso a la red, a la transmisión de datos por redes de telecomunicaciones, a la realización de copia temporal de las páginas de Internet solicitadas por los usuarios, al alojamiento en los propios servidores de información, servicios o aplicaciones facilitados por otros o a la provisión de instrumentos de búsqueda o de enlaces a otros sitios de Internet, así como cualquier otro servicio que se preste a petición individual de los usuarios (descarga de archivos de vídeo o audio...), siempre que represente una actividad económica para el prestador. Estos servicios son ofrecidos por los operadores de telecomunicaciones, los proveedores de acceso a Internet, los portales, los motores de búsqueda o cualquier otro sujeto que disponga de un sitio en Internet a través del que realice alguna de las actividades indicadas, incluido el comercio electrónico.

Desde un punto de vista subjetivo, la Ley se aplica, con carácter general, a los prestadores de servicios establecidos en España. Por "establecimiento" se entiende el lugar desde el que se dirige y gestiona una actividad económica, definición esta que se inspira en el concepto de domicilio fiscal recogido en las normas tributarias españolas y que resulta compatible con la noción material de establecimiento predicada por el Derecho comunitario. La Ley resulta igualmente aplicable a quienes sin ser residentes en España prestan servicios de la sociedad de la información a través de un "establecimiento permanente" situado en España. En este último caso, la sujeción a la Ley es únicamente parcial, respecto a aquellos servicios que se presten desde España.

El lugar de establecimiento del prestador de servicios es un elemento esencial en la Ley, porque de él depende el ámbito de aplicación no sólo de esta Ley, sino de todas las demás disposiciones del ordenamiento español que les sean de aplicación, en función de la actividad que desarrollen. Asimismo, el lugar de establecimiento del prestador determina la ley y las autoridades competentes para el control de su cumplimiento, de acuerdo con el principio de la aplicación de la ley del país de origen que inspira la Directiva 2000/31/CE.

Por lo demás, sólo se permite restringir la libre prestación en España de servicios de la sociedad de la información procedentes de otros países pertenecientes al Espacio Económico Europeo en los supuestos previstos en la Directiva 2000/31/CE, que consisten en la producción de un daño o peligro graves contra ciertos valores fundamentales como el orden público, la salud pública o la protección de los menores. Igualmente, podrá restringirse la prestación de servicios provenientes de dichos Estados cuando afecten a alguna de las materias excluidas del principio de país de origen, que la Ley concreta en su artículo 3, y se incumplan las disposiciones de la normativa española que, en su caso, resulte aplicable a las mismas.

III

Se prevé la anotación del nombre o nombres de dominio de Internet que correspondan al prestador de servicios en el registro público en que, en su caso, dicho prestador conste inscrito para la adquisición de personalidad jurídica o a los solos efectos de publicidad, con el fin de garantizar que la vinculación entre el prestador, su establecimiento físico y su "establecimiento" o localización en la red, que proporciona su dirección de Internet, sea fácilmente accesible para los ciudadanos y la Administración pública.

La Ley establece, asimismo, las obligaciones y responsabilidades de los prestadores de servicios que realicen actividades de intermediación como las de transmisión, copia, alojamiento y localización de datos en la red. En general, éstas imponen a dichos prestadores un deber de colaboración para impedir que determinados servicios o contenidos ilícitos se sigan divulgando. Las responsabilidades que pueden derivar del incumplimiento de estas normas no son sólo de orden administrativo, sino de tipo civil o penal, según los bienes jurídicos afectados y las normas que resulten aplicables.

Destaca, por otra parte, en la Ley, su afán por proteger los intereses de los destinatarios de servicios, de forma que éstos puedan gozar de garantías suficientes a la hora de

contratar un servicio o bien por Internet. Con esta finalidad, la Ley impone a los prestadores de servicios la obligación de facilitar el acceso a sus datos de identificación a cuantos visiten su sitio en Internet; la de informar a los destinatarios sobre los precios que apliquen a sus servicios y la de permitir a éstos visualizar, imprimir y archivar las condiciones generales a que se someta, en su caso, el contrato. Cuando la contratación se efectúe con consumidores, el prestador de servicios deberá, además, guiarles durante el proceso de contratación, indicándoles los pasos que han de dar y la forma de corregir posibles errores en la introducción de datos, y confirmar la aceptación realizada una vez recibida.

En lo que se refiere a las comunicaciones comerciales, la Ley establece que éstas deban identificarse como tales, y prohíbe su envío por correo electrónico u otras vías de comunicación electrónica equivalente, salvo que el destinatario haya prestado su consentimiento.

IV

Se favorece igualmente la celebración de contratos por vía electrónica, al afirmar la Ley, de acuerdo con el principio espiritualista que rige la perfección de los contratos en nuestro Derecho, la validez y eficacia del consentimiento prestado por vía electrónica, declarar que no es necesaria la admisión expresa de esta técnica para que el contrato surta efecto entre las partes, y asegurar la equivalencia entre los documentos en soporte papel y los documentos electrónicos a efectos del cumplimiento del requisito de "forma escrita" que figura en diversas leyes.

Se aprovecha la ocasión para fijar el momento y lugar de celebración de los contratos electrónicos, adoptando una solución única, también válida para otros tipos de contratos celebrados a distancia, que unifica el criterio dispar contenido hasta ahora en los Códigos Civil y de Comercio.

Las disposiciones contenidas en esta Ley sobre aspectos generales de la contratación electrónica, como las relativas a la validez y eficacia de los contratos electrónicos o al momento de prestación del consentimiento, serán de aplicación aun cuando ninguna de las partes tenga la condición de prestador o destinatario de servicios de la sociedad de la información.

La Ley promueve la elaboración de códigos de conducta sobre las materias reguladas en esta Ley, al considerar que son un instrumento de autorregulación especialmente apto para adaptar los diversos preceptos de la Ley a las características específicas de cada sector.

Por su sencillez, rapidez y comodidad para los usuarios, se potencia igualmente el recurso al arbitraje y a los procedimientos alternativos de resolución de conflictos que puedan crearse mediante códigos de conducta, para dirimir las disputas que puedan surgir en la contratación electrónica y en el uso de los demás servicios de la sociedad de la información. Se favorece, además, el uso de medios electrónicos en la tramitación de dichos procedimientos, respetando, en su caso, las normas que, sobre la utilización de dichos medios, establezca la normativa específica sobre arbitraje.

De conformidad con lo dispuesto en las Directivas 2000/31/CE y 98/27/CE, se regula la acción de cesación que podrá ejercitarse para hacer cesar la realización de conductas contrarias a la presente Ley que vulneren los intereses de los consumidores y usuarios. Para el ejercicio de esta acción, deberá tenerse en cuenta, además de lo dispuesto en esta Ley, lo establecido en la Ley general de incorporación de la Directiva 98/27/CE.

La Ley prevé, asimismo, la posibilidad de que los ciudadanos y entidades se dirijan a diferentes Ministerios y órganos administrativos para obtener información práctica sobre distintos aspectos relacionados con las materias objeto de esta Ley, lo que requerirá el establecimiento de mecanismos que aseguren la máxima coordinación entre ellos y la homogeneidad y coherencia de la información suministrada a los usuarios.

Finalmente, se establece un régimen sancionador proporcionado pero eficaz, como indica la Directiva 2000/31/CE, para disuadir a los prestadores de servicios del incumplimiento de lo dispuesto en esta Ley.

Asimismo, se contempla en la Ley una serie de previsiones orientadas a hacer efectiva la accesibilidad de las personas con discapacidad a la información proporcionada por medios electrónicos, y muy especialmente a la información suministrada por las Administraciones

públicas, compromiso al que se refiere la resolución del Consejo de la Unión Europea de 25 de marzo de 2002, sobre accesibilidad de los sitios web públicos y de su contenido.

La presente disposición ha sido elaborada siguiendo un amplio proceso de consulta pública y ha sido sometida al procedimiento de información en materia de normas y reglamentaciones técnicas previsto en la Directiva 98/34/CE, del Parlamento Europeo y del Consejo, de 22 de junio, modificada por la Directiva 98/48/CE, del Parlamento Europeo y del Consejo, de 20 de julio, y en el Real Decreto 1337/1999, de 31 de julio.

TÍTULO I

Disposiciones generales

CAPÍTULO I

Objeto

Artículo 1. *Objeto.*

1. Es objeto de la presente Ley la regulación del régimen jurídico de los servicios de la sociedad de la información y de la contratación por vía electrónica, en lo referente a las obligaciones de los prestadores de servicios incluidos los que actúan como intermediarios en la transmisión de contenidos por las redes de telecomunicaciones, las comunicaciones comerciales por vía electrónica, la información previa y posterior a la celebración de contratos electrónicos, las condiciones relativas a su validez y eficacia y el régimen sancionador aplicable a los prestadores de servicios de la sociedad de la información.

2. Las disposiciones contenidas en esta Ley se entenderán sin perjuicio de lo dispuesto en otras normas estatales o autonómicas ajenas al ámbito normativo coordinado, o que tengan como finalidad la protección de la salud y seguridad pública, incluida la salvaguarda de la defensa nacional, los intereses del consumidor, el régimen tributario aplicable a los servicios de la sociedad de la información, la protección de datos personales y la normativa reguladora de defensa de la competencia.

CAPÍTULO II

Ámbito de aplicación

Artículo 2. *Prestadores de servicios establecidos en España.*

1. Esta Ley será de aplicación a los prestadores de servicios de la sociedad de la información establecidos en España y a los servicios prestados por ellos.

Se entenderá que un prestador de servicios está establecido en España cuando su residencia o domicilio social se encuentren en territorio español, siempre que éstos coincidan con el lugar en que esté efectivamente centralizada la gestión administrativa y la dirección de sus negocios. En otro caso, se atenderá al lugar en que se realice dicha gestión o dirección.

2. Asimismo, esta Ley será de aplicación a los servicios de la sociedad de la información que los prestadores residentes o domiciliados en otro Estado ofrezcan a través de un establecimiento permanente situado en España.

Se considerará que un prestador opera mediante un establecimiento permanente situado en territorio español cuando disponga en el mismo, de forma continuada o habitual, de instalaciones o lugares de trabajo, en los que realice toda o parte de su actividad.

3. A los efectos previstos en este artículo, se presumirá que el prestador de servicios está establecido en España cuando el prestador o alguna de sus sucursales se haya inscrito en el Registro Mercantil o en otro registro público español en el que fuera necesaria la inscripción para la adquisición de personalidad jurídica.

La utilización de medios tecnológicos situados en España, para la prestación o el acceso al servicio, no servirá como criterio para determinar, por sí solo, el establecimiento en España del prestador.

4. Los prestadores de servicios de la sociedad de la información establecidos en España estarán sujetos a las demás disposiciones del ordenamiento jurídico español que les sean de aplicación, en función de la actividad que desarrollen, con independencia de la utilización de medios electrónicos para su realización.

Artículo 3. *Prestadores de servicios establecidos en otro Estado miembro de la Unión Europea o del Espacio Económico Europeo.*

1. Sin perjuicio de lo dispuesto en los artículos 7.1 y 8, esta Ley se aplicará a los prestadores de servicios de la sociedad de la información establecidos en otro Estado miembro de la Unión Europea o del Espacio Económico Europeo cuando el destinatario de los servicios radique en España y los servicios afecten a las materias siguientes:

a) Derechos de propiedad intelectual o industrial.
b) Emisión de publicidad por instituciones de inversión colectiva.
c) Actividad de seguro directo realizada en régimen de derecho de establecimiento o en régimen de libre prestación de servicios.
d) Obligaciones nacidas de los contratos celebrados por personas físicas que tengan la condición de consumidores.
e) Régimen de elección por las partes contratantes de la legislación aplicable a su contrato.
f) Licitud de las comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente no solicitadas.

2. En todo caso, la constitución, transmisión, modificación y extinción de derechos reales sobre bienes inmuebles sitos en España se sujetará a los requisitos formales de validez y eficacia establecidos en el ordenamiento jurídico español.
3. Los prestadores de servicios a los que se refiere el apartado 1 quedarán igualmente sometidos a las normas del ordenamiento jurídico español que regulen las materias señaladas en dicho apartado.
4. No será aplicable lo dispuesto en los apartados anteriores a los supuestos en que, de conformidad con las normas reguladoras de las materias enumeradas en el apartado 1, no fuera de aplicación la ley del país en que resida o esté establecido el destinatario del servicio.

Artículo 4. *Prestadores establecidos en un Estado no perteneciente a la Unión Europea o al Espacio Económico Europeo.*

A los prestadores establecidos en países que no sean miembros de la Unión Europea o del Espacio Económico Europeo, les será de aplicación lo dispuesto en los artículos 7.2 y 11.2.
Los prestadores que dirijan sus servicios específicamente al territorio español quedarán sujetos, además, a las obligaciones previstas en esta Ley, siempre que ello no contravenga lo establecido en tratados o convenios internacionales que sean aplicables.

Artículo 5. *Servicios excluidos del ámbito de aplicación de la Ley.*

1. Se regirán por su normativa específica las siguientes actividades y servicios de la sociedad de la información:

a) Los servicios prestados por notarios y registradores de la propiedad y mercantiles en el ejercicio de sus respectivas funciones públicas.
b) Los servicios prestados por abogados y procuradores en el ejercicio de sus funciones de representación y defensa en juicio.

2. Las disposiciones de la presente Ley, con la excepción de lo establecido en el artículo 7.1, serán aplicables a los servicios de la sociedad de la información relativos a juegos de azar que impliquen apuestas de valor económico, sin perjuicio de lo establecido en su legislación específica estatal o autonómica.

TÍTULO II

Prestación de servicios de la sociedad de la información

CAPÍTULO I

Principio de libre prestación de servicios

Artículo 6. *No sujeción a autorización previa.*

La prestación de servicios de la sociedad de la información no estará sujeta a autorización previa.

Esta norma no afectará a los regímenes de autorización previstos en el ordenamiento jurídico que no tengan por objeto específico y exclusivo la prestación por vía electrónica de los correspondientes servicios.

Artículo 7. *Principio de libre prestación de servicios.*

1. La prestación de servicios de la sociedad de la información que procedan de un prestador establecido en algún Estado miembro de la Unión Europea o del Espacio Económico Europeo se realizará en régimen de libre prestación de servicios, sin que pueda establecerse ningún tipo de restricciones a los mismos por razones derivadas del ámbito normativo coordinado, excepto en los supuestos previstos en los artículos 3 y 8.

2. La aplicación del principio de libre prestación de servicios de la sociedad de la información a prestadores establecidos en Estados no miembros del Espacio Económico Europeo se atendrá a los acuerdos internacionales que resulten de aplicación.

Artículo 8. *Restricciones a la prestación de servicios y procedimiento de cooperación intracomunitario.*

1. En caso de que un determinado servicio de la sociedad de la información atente o pueda atentar contra los principios que se expresan a continuación, los órganos competentes para su protección, en ejercicio de las funciones que tengan legalmente atribuidas, podrán adoptar las medidas necesarias para que se interrumpa su prestación o para retirar los datos que los vulneran. Los principios a que alude este apartado son los siguientes:

a) La salvaguarda del orden público, la investigación penal, la seguridad pública y la defensa nacional.

b) La protección de la salud pública o de las personas físicas o jurídicas que tengan la condición de consumidores o usuarios, incluso cuando actúen como inversores.

c) El respeto a la dignidad de la persona y al principio de no discriminación por motivos de raza, sexo, religión, opinión, nacionalidad, discapacidad o cualquier otra circunstancia personal o social, y

d) La protección de la juventud y de la infancia.

e) La salvaguarda de los derechos de propiedad intelectual.

En la adopción y cumplimiento de las medidas de restricción a que alude este apartado se respetarán, en todo caso, las garantías, normas y procedimientos previstos en el ordenamiento jurídico para proteger los derechos a la intimidad personal y familiar, a la protección de los datos personales, a la libertad de expresión o a la libertad de información, cuando éstos pudieran resultar afectados.

En todos los casos en los que la Constitución y las leyes reguladoras de los respectivos derechos y libertades así lo prevean de forma excluyente, sólo la autoridad judicial competente podrá adoptar las medidas previstas en este artículo, en tanto garante del derecho a la libertad de expresión, del derecho de producción y creación literaria, artística, científica y técnica, la libertad de cátedra y el derecho de información.

2. Los órganos competentes para la adopción de las medidas a que se refiere el apartado anterior, con el objeto de identificar al responsable del servicio de la sociedad de la información que está realizando la conducta presuntamente vulneradora, podrán requerir a los prestadores de servicios de la sociedad de la información la cesión de los datos que

permitan tal identificación a fin de que pueda comparecer en el procedimiento. Tal requerimiento exigirá la previa autorización judicial de acuerdo con lo previsto en el apartado primero del artículo 122 bis de la Ley reguladora de la Jurisdicción contencioso-administrativa. Una vez obtenida la autorización, los prestadores estarán obligados a facilitar los datos necesarios para llevar a cabo la identificación.

3. La adopción de restricciones a la prestación de servicios de la sociedad de la información provenientes de prestadores establecidos en un Estado de la Unión Europea o del Espacio Económico Europeo distinto a España deberá seguir el procedimiento de cooperación intracomunitario descrito en el siguiente apartado de este artículo, sin perjuicio de lo dispuesto en la legislación procesal y de cooperación judicial.

4. Cuando un órgano competente acuerde, en ejercicio de las competencias que tenga legalmente atribuidas, y de acuerdo con lo dispuesto en el párrafo a) del apartado 4 del artículo 3 de la Directiva 2000/31/CE, establecer restricciones que afecten a un servicio de la sociedad de la información que proceda de alguno de los Estados miembros de la Unión Europea o del Espacio Económico Europeo distinto de España, dicho órgano deberá seguir el siguiente procedimiento:

a) El órgano competente requerirá al Estado miembro en que esté establecido el prestador afectado para que adopte las medidas oportunas. En el caso de que no las adopte o resulten insuficientes, dicho órgano notificará, con carácter previo, a la Comisión Europea o, en su caso, al Comité Mixto del Espacio Económico Europeo y al Estado miembro de que se trate las medidas que tiene intención de adoptar.

b) En los supuestos de urgencia, el órgano competente podrá adoptar las medidas oportunas, notificándolas al Estado miembro de procedencia y a la Comisión Europea o, en su caso, al Comité Mixto del Espacio Económico Europeo con la mayor brevedad y, en cualquier caso, como máximo, en el plazo de quince días desde su adopción. Así mismo, deberá indicar la causa de dicha urgencia.

Los requerimientos y notificaciones a que alude este apartado se realizarán siempre a través del órgano de la Administración General del Estado competente para la comunicación y transmisión de información a las Comunidades Europeas.

5. Los órganos competentes de otros Estados Miembros de la Unión Europea o del Espacio Económico Europeo podrán requerir la colaboración de los prestadores de servicios de intermediación establecidos en España en los términos previstos en el apartado 2 del artículo 11 de esta ley si lo estiman necesario para garantizar la eficacia de las medidas de restricción que adopten al amparo del apartado anterior.

6. Las medidas de restricción que se adopten al amparo de este artículo deberán, en todo caso, cumplir las garantías y los requisitos previstos en los apartados 3 y 4 del artículo 11 de esta ley.

CAPÍTULO II

Obligaciones y régimen de responsabilidad de los prestadores de servicios de la sociedad de la información

Sección 1.ª Obligaciones

Artículo 9. *Constancia registral del nombre de dominio.*

(Sin contenido)

Artículo 10. *Información general.*

1. Sin perjuicio de los requisitos que en materia de información se establecen en la normativa vigente, el prestador de servicios de la sociedad de la información estará obligado a disponer de los medios que permitan, tanto a los destinatarios del servicio como a los órganos competentes, acceder por medios electrónicos, de forma permanente, fácil, directa y gratuita, a la siguiente información:

a) Su nombre o denominación social; su residencia o domicilio o, en su defecto, la dirección de uno de sus establecimientos permanentes en España; su dirección de correo electrónico y cualquier otro dato que permita establecer con él una comunicación directa y efectiva.

b) Los datos de su inscripción en el Registro Mercantil en el que, en su caso, se encuentren inscritos o de aquel otro registro público en el que lo estuvieran para la adquisición de personalidad jurídica o a los solos efectos de publicidad.

c) En el caso de que su actividad estuviese sujeta a un régimen de autorización administrativa previa, los datos relativos a dicha autorización y los identificativos del órgano competente encargado de su supervisión.

d) Si ejerce una profesión regulada deberá indicar:

1.º Los datos del Colegio profesional al que, en su caso, pertenezca y número de colegiado.

2.º El título académico oficial o profesional con el que cuente.

3.º El Estado de la Unión Europea o del Espacio Económico Europeo en el que se expidió dicho título y, en su caso, la correspondiente homologación o reconocimiento.

4.º Las normas profesionales aplicables al ejercicio de su profesión y los medios a través de los cuales se puedan conocer, incluidos los electrónicos.

e) El número de identificación fiscal que le corresponda.

f) Cuando el servicio de la sociedad de la información haga referencia a precios, se facilitará información clara y exacta sobre el precio del producto o servicio, indicando si incluye o no los impuestos aplicables y, en su caso, sobre los gastos de envío.

g) Los códigos de conducta a los que, en su caso, esté adherido y la manera de consultarlos electrónicamente.

2. La obligación de facilitar esta información se dará por cumplida si el prestador la incluye en su página o sitio de Internet en las condiciones señaladas en el apartado 1.

3. Cuando se haya atribuido un rango de numeración telefónica a servicios de tarificación adicional en el que se permita el acceso a servicios de la sociedad de la información y se requiera su utilización por parte del prestador de servicios, esta utilización y la descarga de programas informáticos que efectúen funciones de marcación, deberán realizarse con el consentimiento previo, informado y expreso del usuario.

A tal efecto, el prestador del servicio deberá proporcionar al menos la siguiente información:

a) Las características del servicio que se va a proporcionar.

b) Las funciones que efectuarán los programas informáticos que se descarguen, incluyendo el número telefónico que se marcará.

c) El procedimiento para dar fin a la conexión de tarificación adicional, incluyendo una explicación del momento concreto en que se producirá dicho fin, y

d) El procedimiento necesario para restablecer el número de conexión previo a la conexión de tarificación adicional.

La información anterior deberá estar disponible de manera claramente visible e identificable.

Lo dispuesto en este apartado se entiende sin perjuicio de lo establecido en la normativa de telecomunicaciones, en especial, en relación con los requisitos aplicables para el acceso por parte de los usuarios a los rangos de numeración telefónica, en su caso, atribuidos a los servicios de tarificación adicional.

Artículo 11. *Deber de colaboración de los prestadores de servicios de intermediación.*

1. Cuando un órgano competente hubiera ordenado, en ejercicio de las competencias que legalmente tenga atribuidas, que se interrumpa la prestación de un servicio de la sociedad de la información o la retirada de determinados contenidos provenientes de prestadores establecidos en España, y para ello fuera necesaria la colaboración de los prestadores de servicios de intermediación, dicho órgano podrá ordenar a los citados prestadores que suspendan el correspondiente servicio de intermediación utilizado para la

provisión del servicio de la sociedad de la información o de los contenidos cuya interrupción o retirada hayan sido ordenados respectivamente.

2. Si para garantizar la efectividad de la resolución que acuerde la interrupción de la prestación de un servicio o la retirada de contenidos procedentes de un prestador establecido en un Estado no perteneciente a la Unión Europea o al Espacio Económico Europeo, el órgano competente estimara necesario impedir el acceso desde España a los mismos, y para ello fuera necesaria la colaboración de los prestadores de servicios de intermediación establecidos en España, dicho órgano podrá ordenar a los citados prestadores de servicios de intermediación que suspendan el correspondiente servicio de intermediación utilizado para la provisión del servicio de la sociedad de la información o de los contenidos cuya interrupción o retirada hayan sido ordenados respectivamente.

3. En la adopción y cumplimiento de las medidas a que se refieren los apartados anteriores, se respetarán, en todo caso, las garantías, normas y procedimientos previstos en el ordenamiento jurídico para proteger los derechos a la intimidad personal y familiar, a la protección de los datos personales, a la libertad de expresión o a la libertad de información, cuando estos pudieran resultar afectados.

En todos los casos en que la Constitución, las normas reguladoras de los respectivos derechos y libertades o las que resulten aplicables a las diferentes materias atribuyan competencia a los órganos jurisdiccionales de forma excluyente para intervenir en el ejercicio de actividades o derechos, sólo la autoridad judicial competente podrá adoptar las medidas previstas en este artículo. En particular, la autorización del secuestro de páginas de Internet o de su restricción cuando ésta afecte a los derechos y libertades de expresión e información y demás amparados en los términos establecidos en el artículo 20 de la Constitución solo podrá ser decidida por los órganos jurisdiccionales competentes.

4. Las medidas a que hace referencia este artículo serán objetivas, proporcionadas y no discriminatorias, y se adoptarán de forma cautelar o en ejecución de las resoluciones que se dicten, conforme a los procedimientos administrativos legalmente establecidos o a los previstos en la legislación procesal que corresponda.

En particular, cuando resulte necesario para proteger los derechos de la víctima o grupos o personas discriminadas, los jueces y tribunales podrán acordar, de conformidad con la legislación procesal, motivadamente, y siempre de acuerdo con el principio de proporcionalidad, cualquiera de las medidas de restricción o interrupción de la prestación de servicios o de retirada de datos de páginas de internet que contempla la presente ley.

Artículo 12. *Deber de retención de datos de tráfico relativos a las comunicaciones electrónicas.*

(Derogado)

Artículo 12 bis. *Obligaciones de información sobre seguridad.*

1. Los proveedores de servicios de intermediación establecidos en España de acuerdo con lo dispuesto en el artículo 2 de esta Ley que realicen actividades consistentes en la prestación de servicios de acceso a Internet, estarán obligados a informar a sus clientes de forma permanente, fácil, directa y gratuita, sobre los diferentes medios de carácter técnico que aumenten los niveles de la seguridad de la información y permitan, entre otros, la protección frente a virus informáticos y programas espía, y la restricción de los correos electrónicos no solicitados.

2. Los proveedores de servicios de acceso a Internet y los prestadores de servicios de correo electrónico o de servicios similares deberán informar a sus clientes de forma permanente, fácil, directa y gratuita sobre las medidas de seguridad que apliquen en la provisión de los mencionados servicios.

3. Igualmente, los proveedores de servicios referidos en el apartado 1 informarán sobre las herramientas existentes para el filtrado y restricción del acceso a determinados contenidos y servicios en Internet no deseados o que puedan resultar nocivos para la juventud y la infancia.

4. Los proveedores de servicios mencionados en el apartado 1 facilitarán información a sus clientes acerca de las posibles responsabilidades en que puedan incurrir por el uso de

Internet con fines ilícitos, en particular, para la comisión de ilícitos penales y por la vulneración de la legislación en materia de propiedad intelectual e industrial.

5. Las obligaciones de información referidas en los apartados anteriores se darán por cumplidas si el correspondiente proveedor incluye la información exigida en su página o sitio principal de Internet en la forma establecida en los mencionados apartados.

Artículo 12 ter. *Obligaciones relativas a la portabilidad de datos no personales.*

Los proveedores de servicios de intermediación que alojen o almacenen datos de usuarios a los que presten servicios de redes sociales o servicios de la sociedad de la información equivalentes deberán remitir a dichos usuarios, a su solicitud, los contenidos que les hubieran facilitado, sin impedir su transmisión posterior a otro proveedor. La remisión deberá efectuarse en un formato estructurado, de uso común y lectura mecánica.

Asimismo, deberán transmitir dichos contenidos directamente a otro proveedor designado por el usuario, siempre que sea técnicamente posible, según prevé el artículo 95 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.

Para el cumplimiento de estas obligaciones será aplicable lo dispuesto en el artículo 12.5 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

Sección 2.ª Régimen de responsabilidad

Artículo 13. *Responsabilidad de los prestadores de los servicios de la sociedad de la información.*

1. Los prestadores de servicios de la sociedad de la información están sujetos a la responsabilidad civil, penal y administrativa establecida con carácter general en el ordenamiento jurídico, sin perjuicio de lo dispuesto en esta Ley.

2. Para determinar la responsabilidad de los prestadores de servicios por el ejercicio de actividades de intermediación, se estará a lo establecido en los artículos siguientes.

Artículo 14. *Responsabilidad de los operadores de redes y proveedores de acceso.*

1. Los operadores de redes de telecomunicaciones y proveedores de acceso a una red de telecomunicaciones que presten un servicio de intermediación que consista en transmitir por una red de telecomunicaciones datos facilitados por el destinatario del servicio o en facilitar acceso a ésta no serán responsables por la información transmitida, salvo que ellos mismos hayan originado la transmisión, modificado los datos o seleccionado éstos o a los destinatarios de dichos datos.

No se entenderá por modificación la manipulación estrictamente técnica de los archivos que alberguen los datos, que tiene lugar durante su transmisión.

2. Las actividades de transmisión y provisión de acceso a que se refiere el apartado anterior incluyen el almacenamiento automático, provisional y transitorio de los datos, siempre que sirva exclusivamente para permitir su transmisión por la red de telecomunicaciones y su duración no supere el tiempo razonablemente necesario para ello.

Artículo 15. *Responsabilidad de los prestadores de servicios que realizan copia temporal de los datos solicitados por los usuarios.*

Los prestadores de un servicio de intermediación que transmitan por una red de telecomunicaciones datos facilitados por un destinatario del servicio y, con la única finalidad de hacer más eficaz su transmisión ulterior a otros destinatarios que los soliciten, los almacenen en sus sistemas de forma automática, provisional y temporal, no serán responsables por el contenido de esos datos ni por la reproducción temporal de los mismos, si:

a) No modifican la información.

b) Permiten el acceso a ella sólo a los destinatarios que cumplan las condiciones impuestas a tal fin, por el destinatario cuya información se solicita.

c) Respetan las normas generalmente aceptadas y aplicadas por el sector para la actualización de la información.

d) No interfieren en la utilización lícita de tecnología generalmente aceptada y empleada por el sector, con el fin de obtener datos sobre la utilización de la información, y e) Retiran la información que hayan almacenado o hacen imposible el acceso a ella, en cuanto tengan conocimiento efectivo de:

1.º Que ha sido retirada del lugar de la red en que se encontraba inicialmente.

2.º Que se ha imposibilitado el acceso a ella, o 3.º Que un tribunal u órgano administrativo competente ha ordenado retirarla o impedir que se acceda a ella.

Artículo 16. *Responsabilidad de los prestadores de servicios de alojamiento o almacenamiento de datos.*

1. Los prestadores de un servicio de intermediación consistente en albergar datos proporcionados por el destinatario de este servicio no serán responsables por la información almacenada a petición del destinatario, siempre que:

a) No tengan conocimiento efectivo de que la actividad o la información almacenada es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o

b) Si lo tienen, actúen con diligencia para retirar los datos o hacer imposible el acceso a ellos.

Se entenderá que el prestador de servicios tiene el conocimiento efectivo a que se refiere el párrafo a) cuando un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse.

2. La exención de responsabilidad establecida en el apartado 1 no operará en el supuesto de que el destinatario del servicio actúe bajo la dirección, autoridad o control de su prestador.

Artículo 17. *Responsabilidad de los prestadores de servicios que faciliten enlaces a contenidos o instrumentos de búsqueda.*

1. Los prestadores de servicios de la sociedad de la información que faciliten enlaces a otros contenidos o incluyan en los suyos directorios o instrumentos de búsqueda de contenidos no serán responsables por la información a la que dirijan a los destinatarios de sus servicios, siempre que:

a) No tengan conocimiento efectivo de que la actividad o la información a la que remiten o recomiendan es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o

b) Si lo tienen, actúen con diligencia para suprimir o inutilizar el enlace correspondiente.

Se entenderá que el prestador de servicios tiene el conocimiento efectivo a que se refiere el párrafo a) cuando un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse.

2. La exención de responsabilidad establecida en el apartado 1 no operará en el supuesto de que el proveedor de contenidos al que se enlace o cuya localización se facilite actúe bajo la dirección, autoridad o control del prestador que facilite la localización de esos contenidos.

CAPÍTULO III

Códigos de conducta

Artículo 18. *Códigos de conducta.*

1. Las administraciones públicas impulsarán, a través de la coordinación y el asesoramiento, la elaboración y aplicación de códigos de conducta voluntarios, por parte de las corporaciones, asociaciones u organizaciones comerciales, profesionales y de consumidores, en las materias reguladas en esta Ley. La Administración General del Estado fomentará, en especial, la elaboración de códigos de conducta de ámbito comunitario o internacional.

Los códigos de conducta que afecten a los consumidores y usuarios estarán sujetos, además, al capítulo V de la Ley 3/1991, de 10 de enero, de competencia desleal.

Los códigos de conducta podrán tratar, en particular, sobre los procedimientos para la detección y retirada de contenidos ilícitos y la protección de los destinatarios frente al envío por vía electrónica de comunicaciones comerciales no solicitadas, así como sobre los procedimientos extrajudiciales para la resolución de los conflictos que surjan por la prestación de los servicios de la sociedad de la información.

2. En la elaboración de dichos códigos, habrá de garantizarse la participación de las asociaciones de consumidores y usuarios y la de las organizaciones representativas de personas con discapacidades físicas o psíquicas, cuando afecten a sus respectivos intereses.

Cuando su contenido pueda afectarles, los códigos de conducta tendrán especialmente en cuenta la protección de los menores y de la dignidad humana, pudiendo elaborarse, en caso necesario, códigos específicos sobre estas materias.

Los poderes públicos estimularán, en particular, el establecimiento de criterios comunes acordados por la industria para la clasificación y etiquetado de contenidos y la adhesión de los prestadores a los mismos.

3. Los códigos de conducta a los que hacen referencia los apartados precedentes deberán ser accesibles por vía electrónica. Se fomentará su traducción a otras lenguas oficiales, en el Estado y de la Unión Europea, con objeto de darles mayor difusión.

TÍTULO III

Comunicaciones comerciales por vía electrónica

Artículo 19. *Régimen jurídico.*

1. Las comunicaciones comerciales y las ofertas promocionales se regirán, además de por la presente Ley, por su normativa propia y la vigente en materia comercial y de publicidad.

2. En todo caso, será de aplicación la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y su normativa de desarrollo, en especial, en lo que se refiere a la obtención de datos personales, la información a los interesados y la creación y mantenimiento de ficheros de datos personales.

Artículo 20. *Información exigida sobre las comunicaciones comerciales, ofertas promocionales y concursos.*

1. Las comunicaciones comerciales realizadas por vía electrónica deberán ser claramente identificables como tales, y la persona física o jurídica en nombre de la cual se realizan también deberá ser claramente identificable.

2. En los supuestos de ofertas promocionales, como las que incluyan descuentos, premios y regalos, y de concursos o juegos promocionales, previa la correspondiente autorización, se deberá asegurar, además del cumplimiento de los requisitos establecidos en el apartado anterior y en las normas de ordenación del comercio, que queden claramente identificados como tales y que las condiciones de acceso y, en su caso, de participación sean fácilmente accesibles y se expresen de forma clara e inequívoca.

3. Lo dispuesto en los apartados anteriores se entiende sin perjuicio de lo que dispongan las normativas dictadas por las Comunidades Autónomas con competencias exclusivas sobre consumo.

4. En todo caso, queda prohibido el envío de comunicaciones comerciales en las que se disimule o se oculte la identidad del remitente por cuenta de quien se efectúa la comunicación o que contravengan lo dispuesto en este artículo, así como aquéllas en las que se incite a los destinatarios a visitar páginas de Internet que contravengan lo dispuesto en este artículo.

Artículo 21. *Prohibición de comunicaciones comerciales realizadas a través de correo electrónico o medios de comunicación electrónica equivalentes.*

1. Queda prohibido el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas.

2. Lo dispuesto en el apartado anterior no será de aplicación cuando exista una relación contractual previa, siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente.

En todo caso, el prestador deberá ofrecer al destinatario la posibilidad de oponerse al tratamiento de sus datos con fines promocionales mediante un procedimiento sencillo y gratuito, tanto en el momento de recogida de los datos como en cada una de las comunicaciones comerciales que le dirija.

Cuando las comunicaciones hubieran sido remitidas por correo electrónico, dicho medio deberá consistir necesariamente en la inclusión de una dirección de correo electrónico u otra dirección electrónica válida donde pueda ejercitarse este derecho, quedando prohibido el envío de comunicaciones que no incluyan dicha dirección.

Artículo 22. *Derechos de los destinatarios de servicios.*

1. El destinatario podrá revocar en cualquier momento el consentimiento prestado a la recepción de comunicaciones comerciales con la simple notificación de su voluntad al remitente.

A tal efecto, los prestadores de servicios deberán habilitar procedimientos sencillos y gratuitos para que los destinatarios de servicios puedan revocar el consentimiento que hubieran prestado. Cuando las comunicaciones hubieran sido remitidas por correo electrónico dicho medio deberá consistir necesariamente en la inclusión de una dirección de correo electrónico u otra dirección electrónica válida donde pueda ejercitarse este derecho quedando prohibido el envío de comunicaciones que no incluyan dicha dirección.

Asimismo, deberán facilitar información accesible por medios electrónicos sobre dichos procedimientos.

2. Los prestadores de servicios podrán utilizar dispositivos de almacenamiento y recuperación de datos en equipos terminales de los destinatarios, a condición de que los mismos hayan dado su consentimiento después de que se les haya facilitado información clara y completa sobre su utilización, en particular, sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

Cuando sea técnicamente posible y eficaz, el consentimiento del destinatario para aceptar el tratamiento de los datos podrá facilitarse mediante el uso de los parámetros adecuados del navegador o de otras aplicaciones.

Lo anterior no impedirá el posible almacenamiento o acceso de índole técnica al solo fin de efectuar la transmisión de una comunicación por una red de comunicaciones electrónicas o, en la medida que resulte estrictamente necesario, para la prestación de un servicio de la sociedad de la información expresamente solicitado por el destinatario.

TÍTULO IV

Contratación por vía electrónica

Artículo 23. *Validez y eficacia de los contratos celebrados por vía electrónica.*

1. Los contratos celebrados por vía electrónica producirán todos los efectos previstos por el ordenamiento jurídico, cuando concurran el consentimiento y los demás requisitos necesarios para su validez.

Los contratos electrónicos se regirán por lo dispuesto en este Título, por los Códigos Civil y de Comercio y por las restantes normas civiles o mercantiles sobre contratos, en especial, las normas de protección de los consumidores y usuarios y de ordenación de la actividad comercial.

2. Para que sea válida la celebración de contratos por vía electrónica no será necesario el previo acuerdo de las partes sobre la utilización de medios electrónicos.

3. Siempre que la Ley exija que el contrato o cualquier información relacionada con el mismo conste por escrito, este requisito se entenderá satisfecho si el contrato o la información se contiene en un soporte electrónico.

4. No será de aplicación lo dispuesto en el presente Título a los contratos relativos al Derecho de familia y sucesiones.

Los contratos, negocios o actos jurídicos en los que la Ley determine para su validez o para la producción de determinados efectos la forma documental pública, o que requieran por Ley la intervención de órganos jurisdiccionales, notarios, registradores de la propiedad y mercantiles o autoridades públicas, se regirán por su legislación específica.

Artículo 24. *Prueba de los contratos celebrados por vía electrónica.*

1. La prueba de la celebración de un contrato por vía electrónica y la de las obligaciones que tienen su origen en él se sujetará a las reglas generales del ordenamiento jurídico.

Cuando los contratos celebrados por vía electrónica estén firmados electrónicamente se estará a lo establecido en el artículo 3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

2. En todo caso, el soporte electrónico en que conste un contrato celebrado por vía electrónica será admisible en juicio como prueba documental.

Artículo 25. *Intervención de terceros de confianza.*

(Derogado)

Artículo 26. *Ley aplicable.*

Para la determinación de la ley aplicable a los contratos electrónicos se estará a lo dispuesto en las normas de Derecho internacional privado del ordenamiento jurídico español, debiendo tomarse en consideración para su aplicación lo establecido en los artículos 2 y 3 de esta Ley.

Artículo 27. *Obligaciones previas a la contratación.*

1. Además del cumplimiento de los requisitos en materia de información que se establecen en la normativa vigente, el prestador de servicios de la sociedad de la información que realice actividades de contratación electrónica tendrá la obligación de poner a disposición del destinatario, antes de iniciar el procedimiento de contratación y mediante técnicas adecuadas al medio de comunicación utilizado, de forma permanente, fácil y gratuita, información clara, comprensible e inequívoca sobre los siguientes extremos:

a) Los distintos trámites que deben seguirse para celebrar el contrato.

b) Si el prestador va a archivar el documento electrónico en que se formalice el contrato y si éste va a ser accesible.

c) Los medios técnicos que pone a su disposición para identificar y corregir errores en la introducción de los datos, y

d) La lengua o lenguas en que podrá formalizarse el contrato.

La obligación de poner a disposición del destinatario la información referida en el párrafo anterior se dará por cumplida si el prestador la incluye en su página o sitio de Internet en las condiciones señaladas en dicho párrafo.

Cuando el prestador diseñe específicamente sus servicios de contratación electrónica para ser accedidos mediante dispositivos que cuenten con pantallas de formato reducido, se entenderá cumplida la obligación establecida en este apartado cuando facilite de manera permanente, fácil, directa y exacta la dirección de Internet en que dicha información es puesta a disposición del destinatario.

2. El prestador no tendrá la obligación de facilitar la información señalada en el apartado anterior cuando:

a) Ambos contratantes así lo acuerden y ninguno de ellos tenga la consideración de consumidor, o

b) El contrato se haya celebrado exclusivamente mediante intercambio de correo electrónico u otro tipo de comunicación electrónica equivalente.

3. Sin perjuicio de lo dispuesto en la legislación específica, las ofertas o propuestas de contratación realizadas por vía electrónica serán válidas durante el período que fije el oferente o, en su defecto, durante todo el tiempo que permanezcan accesibles a los destinatarios del servicio.

4. Con carácter previo al inicio del procedimiento de contratación, el prestador de servicios deberá poner a disposición del destinatario las condiciones generales a que, en su caso, deba sujetarse el contrato, de manera que éstas puedan ser almacenadas y reproducidas por el destinatario.

Artículo 28. *Información posterior a la celebración del contrato.*

1. El oferente está obligado a confirmar la recepción de la aceptación al que la hizo por alguno de los siguientes medios:

a) El envío de un acuse de recibo por correo electrónico u otro medio de comunicación electrónica equivalente a la dirección que el aceptante haya señalado, en el plazo de las veinticuatro horas siguientes a la recepción de la aceptación, o

b) La confirmación, por un medio equivalente al utilizado en el procedimiento de contratación, de la aceptación recibida, tan pronto como el aceptante haya completado dicho procedimiento, siempre que la confirmación pueda ser archivada por su destinatario.

En los casos en que la obligación de confirmación corresponda a un destinatario de servicios, el prestador facilitará el cumplimiento de dicha obligación, poniendo a disposición del destinatario alguno de los medios indicados en este apartado. Esta obligación será exigible tanto si la confirmación debiera dirigirse al propio prestador o a otro destinatario.

2. Se entenderá que se ha recibido la aceptación y su confirmación cuando las partes a que se dirijan puedan tener constancia de ello.

En el caso de que la recepción de la aceptación se confirme mediante acuse de recibo, se presumirá que su destinatario puede tener la referida constancia desde que aquél haya sido almacenado en el servidor en que esté dada de alta su cuenta de correo electrónico, o en el dispositivo utilizado para la recepción de comunicaciones.

3. No será necesario confirmar la recepción de la aceptación de una oferta cuando:

a) Ambos contratantes así lo acuerden y ninguno de ellos tenga la consideración de consumidor, o

b) El contrato se haya celebrado exclusivamente mediante intercambio de correo electrónico u otro tipo de comunicación electrónica equivalente, cuando estos medios no sean empleados con el exclusivo propósito de eludir el cumplimiento de tal obligación.

Artículo 29. *Lugar de celebración del contrato.*

Los contratos celebrados por vía electrónica en los que intervenga como parte un consumidor se presumirán celebrados en el lugar en que éste tenga su residencia habitual.

Los contratos electrónicos entre empresarios o profesionales, en defecto de pacto entre las partes, se presumirán celebrados en el lugar en que esté establecido el prestador de servicios.

TÍTULO V

Solución judicial y extrajudicial de conflictos

CAPÍTULO I

Acción de cesación

Artículo 30. *Acción de cesación.*

1. Contra las conductas contrarias a la presente Ley que lesionen intereses colectivos o difusos de los consumidores podrá interponerse acción de cesación.
2. La acción de cesación se dirige a obtener una sentencia que condene al demandado a cesar en la conducta contraria a la presente Ley y a prohibir su reiteración futura. Asimismo, la acción podrá ejercerse para prohibir la realización de una conducta cuando ésta haya finalizado al tiempo de ejercitar la acción, si existen indicios suficientes que hagan temer su reiteración de modo inminente.
3. La acción de cesación se ejercerá conforme a las prescripciones de la Ley de Enjuiciamiento Civil para esta clase de acciones.

Artículo 31. *Legitimación activa.*

Están legitimados para interponer la acción de cesación:

a) Las personas físicas o jurídicas titulares de un derecho o interés legítimo, incluidas aquéllas que pudieran verse perjudicadas por infracciones de las disposiciones contenidas en los artículos 21 y 22, entre ellas, los proveedores de servicios de comunicaciones electrónicas que deseen proteger sus intereses comerciales legítimos o los intereses de sus clientes.
b) Los grupos de consumidores o usuarios afectados, en los casos y condiciones previstos en la Ley de Enjuiciamiento Civil.
c) Las asociaciones de consumidores y usuarios que reúnan los requisitos establecidos en la Ley 26/1984, de 19 de julio, General para la Defensa de los Consumidores y Usuarios, o, en su caso, en la legislación autonómica en materia de defensa de los consumidores.
d) El Ministerio Fiscal.
e) El Instituto Nacional del Consumo y los órganos correspondientes de las Comunidades Autónomas y de las Corporaciones Locales competentes en materia de defensa de los consumidores.
f) Las entidades de otros Estados miembros de la Unión Europea constituidas para la protección de los intereses colectivos o difusos de los consumidores que estén habilitadas ante la Comisión Europea mediante su inclusión en la lista publicada a tal fin en el "Diario Oficial de las Comunidades Europeas".
Los Jueces y Tribunales aceptarán dicha lista como prueba de la capacidad de la entidad habilitada para ser parte, sin perjuicio de examinar si la finalidad de la misma y los intereses afectados legitiman el ejercicio de la acción.

CAPÍTULO II

Solución extrajudicial de conflictos

Artículo 32. *Solución extrajudicial de conflictos.*

1. El prestador y el destinatario de servicios de la sociedad de la información podrán someter sus conflictos a los arbitrajes previstos en la legislación de arbitraje y de defensa de los consumidores y usuarios, y a los procedimientos de resolución extrajudicial de conflictos que se instauren por medio de códigos de conducta u otros instrumentos de autorregulación.

2. En los procedimientos de resolución extrajudicial de conflictos a que hace referencia el apartado anterior, podrá hacerse uso de medios electrónicos, en los términos que establezca su normativa específica.

TÍTULO VI

Información y control

Artículo 33. *Información a los destinatarios y prestadores de servicios.*

Los destinatarios y prestadores de servicios de la sociedad de la información podrán dirigirse a cualesquiera órganos competentes en materia de sociedad de la información, sanidad y consumo de las Administraciones Públicas, para:

a) Conseguir información general sobre sus derechos y obligaciones contractuales en el marco de la normativa aplicable a la contratación electrónica,

b) Informarse sobre los procedimientos de resolución judicial y extrajudicial de conflictos, y

c) Obtener los datos de las autoridades, asociaciones u organizaciones que puedan facilitarles información adicional o asistencia práctica.

La comunicación con dichos órganos podrá hacerse por medios electrónicos.

Artículo 34. *Comunicación de resoluciones relevantes.*

1. El Consejo General del Poder Judicial remitirá al Ministerio de Justicia, en la forma y con la periodicidad que se acuerde mediante Convenio entre ambos órganos, todas las resoluciones judiciales que contengan pronunciamientos relevantes sobre la validez y eficacia de los contratos celebrados por vía electrónica, sobre su utilización como prueba en juicio, o sobre los derechos, obligaciones y régimen de responsabilidad de los destinatarios y los prestadores de servicios de la sociedad de la información.

2. Los órganos arbitrales y los responsables de los demás procedimientos de resolución extrajudicial de conflictos a que se refiere el artículo 32.1 comunicarán al Ministerio de Justicia los laudos o decisiones que revistan importancia para la prestación de servicios de la sociedad de la información y el comercio electrónico de acuerdo con los criterios indicados en el apartado anterior.

3. En la comunicación de las resoluciones, laudos y decisiones a que se refiere este artículo, se tomarán las precauciones necesarias para salvaguardar el derecho a la intimidad y a la protección de los datos personales de las personas identificadas en ellos.

4. El Ministerio de Justicia remitirá a la Comisión Europea y facilitará el acceso de cualquier interesado a la información recibida de conformidad con este artículo.

Artículo 35. *Supervisión y control.*

1. El Ministerio de Asuntos Económicos y Transformación Digital controlará:

a) El cumplimiento por los prestadores de servicios de la sociedad de la información de las obligaciones establecidas en esta Ley y en sus disposiciones de desarrollo, en lo que se refiere a los servicios propios de la sociedad de la información.

b) El cumplimiento de las obligaciones establecidas en el Reglamento (UE) 2019/1150 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, sobre el fomento de la equidad y la transparencia para los usuarios profesionales de servicios de intermediación en línea, por parte de aquellos proveedores incluidos en su ámbito de aplicación.

c) El cumplimiento de las obligaciones establecidas en el Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022, relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 por parte de proveedores de servicios de intermediación de datos y organizaciones reconocidas de gestión de datos con fines altruistas incluidos en su ámbito de aplicación.

No obstante, las referencias a los órganos competentes contenidas en los artículos 8, 10, 11, 15, 16, 17 y 38 se entenderán hecha a los órganos jurisdiccionales o administrativos que, en cada caso, lo sean en función de la materia.

2. Los órganos citados en el apartado 1 de este artículo podrán realizar las actuaciones inspectoras que sean precisas para el ejercicio de su función de control.

Los funcionarios adscritos a dichos órganos y que ejerzan la inspección a que se refiere el párrafo anterior tendrán la consideración de autoridad pública en el desempeño de sus cometidos.

3. En todo caso, y no obstante lo dispuesto en el apartado anterior, cuando las conductas realizadas por los prestadores de servicios de la sociedad de la información estuvieran sujetas, por razón de la materia o del tipo de entidad de que se trate, a ámbitos competenciales, de tutela o de supervisión específicos, con independencia de que se lleven a cabo utilizando técnicas y medios telemáticos o electrónicos, los órganos a los que la legislación sectorial atribuya competencias de control, supervisión, inspección o tutela específica ejercerán las funciones que les correspondan.

Artículo 35 bis. *Registro nacional de organizaciones reconocidas de gestión de datos con fines altruistas.*

1. El Ministerio de Asuntos Económicos y Transformación Digital establecerá, mantendrá y publicará el registro nacional de organizaciones reconocidas de gestión de datos con fines altruistas, según lo previsto en el artículo 17 del Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022, relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724.

2. El plazo máximo para dictar y notificar resolución en el procedimiento de verificación previa de cumplimiento de los requisitos establecidos en el citado Reglamento (UE) 2022/868 para la inscripción en el registro de las organizaciones de gestión de datos con fines altruistas será de 12 semanas, transcurridas las cuales se podrá entender desestimada la solicitud.

Artículo 36. *Deber de colaboración.*

1. Los prestadores de servicios de la sociedad de la información tienen la obligación de facilitar al Ministerio de Ciencia y Tecnología y a los demás órganos a que se refiere el artículo anterior toda la información y colaboración precisas para el ejercicio de sus funciones.

Igualmente, deberán permitir a sus agentes o al personal inspector el acceso a sus instalaciones y la consulta de cualquier documentación relevante para la actividad de control de que se trate, siendo de aplicación, en su caso, lo dispuesto en el artículo 8.5 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa.

2. Cuando, como consecuencia de una actuación inspectora, se tuviera conocimiento de hechos que pudieran ser constitutivos de infracciones tipificadas en otras leyes, estatales o autonómicas, se dará cuenta de los mismos a los órganos u organismos competentes para su supervisión y sanción.

Artículo 36 bis. *Deber de comunicación de las organizaciones y asociaciones representativas de usuarios profesionales o de los usuarios de sitios web corporativos.*

Las organizaciones y asociaciones que posean un interés legítimo de representación de usuarios profesionales o de los usuarios de sitios web corporativos, y que, cumpliendo con los requisitos del artículo 14.3 del Reglamento (UE) 2019/1150, hubieren solicitado al Ministerio de Asuntos Económicos y Transformación Digital su inclusión en la lista elaborada al efecto por la Comisión Europea, notificarán inmediatamente al citado Ministerio cualquier circunstancia que afecte a su entidad que derive en un incumplimiento sobrevenido de los mencionados requisitos.

TÍTULO VII

Infracciones y sanciones

Artículo 37. *Responsables.*

Están sujetos al régimen sancionador establecido en este título:

a) Los prestadores de servicios de la sociedad de la información a los que les sea de aplicación la presente Ley.
b) Los proveedores incluidos en el ámbito de aplicación del Reglamento (UE) 2019/1150.
c) Los proveedores de servicios de intermediación de datos y las organizaciones reconocidas de gestión de datos con fines altruistas incluidos en el ámbito de aplicación del Reglamento (UE) 2022/868.

Cuando las infracciones previstas en el artículo 38.3 i) y 38.4 g) se deban a la instalación de dispositivos de almacenamiento y recuperación de la información como consecuencia de la cesión por parte del prestador del servicio de la sociedad de la información de espacios propios para mostrar publicidad, será responsable de la infracción, además del prestador del servicio de la sociedad de la información, la red publicitaria o agente que gestione directamente con aquel la colocación de anuncios en dichos espacios en caso de no haber adoptado medidas para exigirle el cumplimiento de los deberes de información y la obtención del consentimiento del usuario.

Artículo 38. *Infracciones.*

1. Las infracciones de los preceptos de esta Ley se calificarán como muy graves, graves y leves.
2. Son infracciones muy graves:

a) **(Sin contenido)**
b) El incumplimiento de la obligación de suspender la transmisión, el alojamiento de datos, el acceso a la red o la prestación de cualquier otro servicio equivalente de intermediación, cuando un órgano administrativo competente lo ordene, en virtud de lo dispuesto en el artículo 11.
c) **(Derogado)**
d) **(Derogado)**

3. Son infracciones graves:

a) **(Derogado)**
b) El incumplimiento significativo de lo establecido en los párrafos a) y f) del artículo 10.1.
c) El envío masivo de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente, o su envío insistente o sistemático a un mismo destinatario del servicio cuando en dichos envíos no se cumplan los requisitos establecidos en el artículo 21.
d) El incumplimiento significativo de la obligación del prestador de servicios establecida en el apartado 1 del artículo 22, en relación con los procedimientos para revocar el consentimiento prestado por los destinatarios.
e) No poner a disposición del destinatario del servicio las condiciones generales a que, en su caso, se sujete el contrato, en la forma prevista en el artículo 27.
f) El incumplimiento habitual de la obligación de confirmar la recepción de una aceptación, cuando no se haya pactado su exclusión o el contrato se haya celebrado con un consumidor.
g) La resistencia, excusa o negativa a la actuación inspectora de los órganos facultados para llevarla a cabo con arreglo a esta ley.
h) El incumplimiento significativo de lo establecido en el apartado 3 del artículo 10.
i) La reincidencia en la comisión de la infracción leve prevista en el apartado 4 g) cuando así se hubiera declarado por resolución firme dictada en los tres años inmediatamente anteriores a la apertura del procedimiento sancionador.
j) La exigencia del pago de un canon por atender la obligación prevista en el artículo 12 ter, fuera de los supuestos establecidos en el artículo 12.5 del Reglamento (UE) 2016/679.

k) El incumplimiento habitual de la obligación prevista en el artículo 12 ter.

l) El incumplimiento significativo o reiterado por parte de los proveedores de servicios de intermediación en línea de cualquiera de las obligaciones establecidas en los artículos 3 a 12 del Reglamento (UE) 2019/1150.

m) El incumplimiento significativo o reiterado por parte de los proveedores de motores de búsqueda en línea de cualquiera de las obligaciones establecidas en los artículos 5 y 7 del Reglamento (UE) 2019/1150.

n) El incumplimiento significativo o reiterado por parte de los proveedores de servicios de intermediación de datos de cualquiera de las obligaciones previstas en el artículo 11 del Reglamento (UE) 2022/868.

ñ) El incumplimiento significativo o reiterado por parte de los proveedores de servicios de intermediación de datos de cualquiera de las condiciones para la prestación de servicios de intermediación de datos establecidas en el artículo 12 del Reglamento (UE) 2022/868.

o) Actuar en el mercado como proveedor de servicios de intermediación de datos utilizando el logotipo común y la denominación «proveedor de servicios de intermediación de datos reconocido en la Unión» sin que la autoridad competente haya confirmado que cumple los requisitos necesarios según lo previsto en el artículo 11.9 del Reglamento (UE) 2022/868.

p) El incumplimiento significativo o reiterado por parte de las organizaciones reconocidas de gestión de datos con fines altruistas de cualquiera de los requisitos exigidos en virtud de los artículos 18, 19, 20, 21 y 22 del Reglamento (UE) 2022/868.

q) Actuar en el mercado como organización reconocida de gestión de datos con fines altruistas utilizando el logotipo común y la denominación «organización de gestión de datos con fines altruistas reconocida en la Unión» sin que la autoridad competente haya confirmado que cumple los requisitos necesarios previstos en el artículo 18 del Reglamento (UE) 2022/868.

r) El incumplimiento significativo o reiterado por parte de proveedores de servicios de intermediación de datos y de organizaciones reconocidas de gestión de datos con fines altruistas de las obligaciones establecidas en el artículo 31 del Reglamento (UE) 2022/868 en materia de transferencias de datos no personales a terceros países.

4. Son infracciones leves:

a) El incumplimiento de lo previsto en el artículo 12 bis.

b) No informar en la forma prescrita por el artículo 10.1 sobre los aspectos señalados en los párrafos b), c), d), e) y g) del mismo, o en los párrafos a) y f) cuando no constituya infracción grave.

c) El incumplimiento de lo previsto en el artículo 20 para las comunicaciones comerciales, ofertas promocionales y concursos.

d) El envío de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente cuando en dichos envíos no se cumplan los requisitos establecidos en el artículo 21 y no constituya infracción grave.

e) No facilitar la información a que se refiere el artículo 27.1, cuando las partes no hayan pactado su exclusión o el destinatario sea un consumidor.

f) El incumplimiento de la obligación de confirmar la recepción de una petición en los términos establecidos en el artículo 28, cuando no se haya pactado su exclusión o el contrato se haya celebrado con un consumidor, salvo que constituya infracción grave.

g) Utilizar dispositivos de almacenamiento y recuperación de datos cuando no se hubiera facilitado la información u obtenido el consentimiento del destinatario del servicio en los términos exigidos por el artículo 22.2.

h) El incumplimiento de la obligación del prestador de servicios establecida en el apartado 1 del artículo 22, en relación con los procedimientos para revocar el consentimiento prestado por los destinatarios cuando no constituya infracción grave.

i) El incumplimiento de lo establecido en el apartado 3 del artículo 10, cuando no constituya infracción grave.

j) La exigencia del pago de un canon por atender la obligación prevista en el artículo 12 ter, cuando así lo permita el artículo 12.5 del Reglamento (UE) 2016/679, si su cuantía excediese el importe de los costes afrontados.

k) El incumplimiento de la obligación prevista en el artículo 12 ter, cuando no constituya infracción grave.

l) El incumplimiento por parte de los proveedores de servicios de intermediación en línea de cualquiera de las obligaciones establecidas en los artículos 3 a 12 del Reglamento (UE) 2019/1150, cuando no constituya infracción grave.

m) El incumplimiento por parte de los proveedores de motores de búsqueda en línea de cualquiera de las obligaciones establecidas en los artículos 5 y 7 del Reglamento (UE) 2019/1150, cuando no constituya infracción grave.

n) El incumplimiento por parte de los proveedores de servicios de intermediación de datos de cualquiera de las obligaciones previstas en el artículo 11 del Reglamento (UE) 2022/868, cuando no constituya infracción grave.

ñ) El incumplimiento por parte de los proveedores de servicios de intermediación de datos de cualquiera de las condiciones establecidas en el artículo 12 del Reglamento (UE) 2022/868, cuando no constituya infracción grave.

o) El incumplimiento por parte de las organizaciones reconocidas de gestión de datos con fines altruistas de cualquiera de los requisitos exigidos en virtud de los artículos 18, 19, 20, 21 y 22 del Reglamento (UE) 2022/868, cuando no constituya infracción grave.

p) El incumplimiento por parte de proveedores de servicios de intermediación de datos y de organizaciones reconocidas de gestión de datos con fines altruistas de las obligaciones establecidas en el artículo 31 del Reglamento (UE) 2022/868 en materia de transferencias de datos no personales a terceros países, cuando no constituya infracción grave.

Artículo 39. *Sanciones.*

1. Por la comisión de las infracciones recogidas en el artículo anterior, se impondrán las siguientes sanciones:

a) Por la comisión de infracciones muy graves, multa de 150.001 hasta 600.000 euros. La reiteración en el plazo de tres años de dos o más infracciones muy graves, sancionadas con carácter firme, podrá dar lugar, en función de sus circunstancias, a la sanción de prohibición de actuación en España, durante un plazo máximo de dos años.

b) comisión de infracciones graves, multa de 30.001 hasta 150.000 euros.

c) Por la comisión de infracciones leves, multa de hasta 30.000 euros.

2. Cuando las infracciones sancionables con arreglo a lo previsto en esta Ley hubieran sido cometidas por prestadores de servicios establecidos en Estados que no sean miembros de la Unión Europea o del Espacio Económico Europeo, el órgano que hubiera impuesto la correspondiente sanción podrá ordenar a los prestadores de servicios de intermediación que tomen las medidas necesarias para impedir el acceso desde España a los servicios ofrecidos por aquéllos por un período máximo de dos años en el caso de infracciones muy graves, un año en el de infracciones graves y seis meses en el de infracciones leves.

3. Sin perjuicio de las sanciones económicas que pudieran imponerse con arreglo a esta ley, por la comisión de la infracción prevista en la letra p) del apartado 3 del artículo 38, o la letra o) del apartado 4 del artículo 38, se cancelará la inscripción en los registros públicos nacional y de la Unión de organizaciones reconocidas de gestión de datos con fines altruistas, así como se revocará el derecho a utilizar la denominación organización de gestión de datos con fines altruistas reconocida en la Unión.

4. Las infracciones podrán llevar aparejada alguna o algunas de las siguientes sanciones accesorias:

a) Las infracciones graves y muy graves podrán llevar aparejada la publicación, a costa del sancionado, de la resolución sancionadora en el "Boletín Oficial del Estado", o en el diario oficial de la administración pública que, en su caso, hubiera impuesto la sanción; en dos periódicos cuyo ámbito de difusión coincida con el de actuación de la citada administración pública o en la página de inicio del sitio de Internet del prestador, una vez que aquélla tenga carácter firme.

Para la imposición de esta sanción, se considerará la repercusión social de la infracción cometida, por el número de usuarios o de contratos afectados, y la gravedad del ilícito.

b) Sin perjuicio de las sanciones económicas a las que se refiere el artículo 39.1 b), a los prestadores de servicios de intermediación de datos que hayan cometido alguna de las

infracciones graves previstas en las letras n), ñ) y o) del artículo 38.3, se les podrá imponer como sanción accesoria el cese definitivo de la actividad de prestación en los términos establecidos en el artículo 14.4 del Reglamento (UE) 2022/868.

Artículo 39 bis. *Moderación de las sanciones.*

El órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate, en los siguientes supuestos:

a) Cuando se aprecie una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho como consecuencia de la concurrencia significativa de varios de los criterios enunciados en el artículo 40.
b) Cuando la entidad infractora haya regularizado la situación irregular de forma diligente.
c) Cuando pueda apreciarse que la conducta del afectado ha podido inducir a la comisión de la infracción.
d) Cuando el infractor haya reconocido espontáneamente su culpabilidad.
e) Cuando se haya producido un proceso de fusión por absorción y la infracción fuese anterior a dicho proceso, no siendo imputable a la entidad absorbente.

Artículo 39 ter. *Apercibimiento.*

1. Los órganos con competencia sancionadora, atendida la naturaleza de los hechos y la concurrencia significativa de los criterios establecidos en los artículos 39 bis y 40, podrán acordar no iniciar la apertura del procedimiento sancionador y, en su lugar, apercibir al sujeto responsable, a fin de que en el plazo que el órgano sancionador determine, acredite la adopción de las medidas correctoras que, en cada caso, resulten pertinentes, siempre que los hechos fuesen constitutivos de infracción leve o grave conforme a lo dispuesto en esta Ley.
2. Si el apercibimiento no fuera atendido en el plazo que el órgano sancionador hubiera determinado, procederá la apertura del correspondiente procedimiento sancionador por dicho incumplimiento.

Artículo 40. *Graduación de la cuantía de las sanciones.*

La cuantía de las multas que se impongan se graduará atendiendo a los siguientes criterios:

a) La existencia de intencionalidad.
b) Plazo de tiempo durante el que se haya venido cometiendo la infracción.
c) La reincidencia por comisión de infracciones de la misma naturaleza, cuando así haya sido declarado por resolución firme.
d) La naturaleza y cuantía de los perjuicios causados.
e) Los beneficios obtenidos por la infracción.
f) Volumen de facturación a que afecte la infracción cometida.
g) La adhesión a un código de conducta o a un sistema de autorregulación publicitaria aplicable respecto a la infracción cometida, que cumpla con lo dispuesto en el artículo 18 o en la disposición final octava y que haya sido informado favorablemente por el órgano u órganos competentes.
h) La adopción de medidas para mitigar o reparar el daño causado por la infracción.

Artículo 41. *Medidas de carácter provisional.*

1. En los procedimientos sancionadores por infracciones graves o muy graves se podrán adoptar, con arreglo a la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, y sus normas de desarrollo, las medidas de carácter provisional previstas en dichas normas que se estimen necesarias para asegurar la eficacia de la resolución que definitivamente se dicte, el buen fin del procedimiento, evitar el mantenimiento de los efectos de la infracción y las exigencias de los intereses generales.

En particular, podrán acordarse las siguientes:

a) Suspensión temporal de la actividad del prestador de servicios y, en su caso, cierre provisional de sus establecimientos.

b) Precinto, depósito o incautación de registros, soportes y archivos informáticos y de documentos en general, así como de aparatos y equipos informáticos de todo tipo.

c) Advertir al público de la existencia de posibles conductas infractoras y de la incoación del expediente sancionador de que se trate, así como de las medidas adoptadas para el cese de dichas conductas.

2. En la adopción y cumplimiento de las medidas a que se refiere el apartado anterior, se respetarán, en todo caso, las garantías, normas y procedimientos previstos en el ordenamiento jurídico para proteger los derechos a la intimidad personal y familiar, a la protección de los datos personales, a la libertad de expresión o a la libertad de información, cuando éstos pudieran resultar afectados.

En todos los casos en que la Constitución, las normas reguladoras de los respectivos derechos y libertades o las que resulten aplicables a las diferentes materias atribuyan competencia a los órganos jurisdiccionales para intervenir en el ejercicio de actividades o derechos, sólo la autoridad judicial competente podrá adoptar las medidas previstas en este artículo.

3. En todo caso, se respetará el principio de proporcionalidad de la medida a adoptar con los objetivos que se pretendan alcanzar en cada supuesto.

4. En casos de urgencia y para la inmediata protección de los intereses implicados, las medidas provisionales previstas en el presente artículo podrán ser acordadas antes de la iniciación del expediente sancionador. Las medidas deberán ser confirmadas, modificadas o levantadas en el acuerdo de iniciación del procedimiento, que deberá efectuarse dentro de los quince días siguientes a su adopción, el cual podrá ser objeto del recurso que proceda.

En todo caso, dichas medidas quedarán sin efecto si no se inicia el procedimiento sancionador en dicho plazo o cuando el acuerdo de iniciación no contenga un pronunciamiento expreso acerca de las mismas.

Artículo 42. *Multa coercitiva.*

El órgano administrativo competente para resolver el procedimiento sancionador podrá imponer multas coercitivas por importe que no exceda de 6.000 euros por cada día que transcurra sin cumplir las medidas provisionales que hubieran sido acordadas.

Artículo 43. *Competencia sancionadora.*

1. La imposición de sanciones por el incumplimiento de lo previsto en esta Ley corresponderá, en el caso de infracciones muy graves, a la persona titular del Ministerio de Asuntos Económicos y Transformación Digital, y en el de infracciones graves y leves, a la persona titular de la Secretaria de Estado de Digitalización e Inteligencia Artificial.

No obstante lo anterior, la imposición de sanciones por incumplimiento de las resoluciones dictadas por los órganos competentes en función de la materia o entidad de que se trate a que se refieren las letras a) y b) del artículo 38.2 de esta Ley corresponderá al órgano que dictó la resolución incumplida. Igualmente, corresponderá a la Agencia de Protección de Datos la imposición de sanciones por la comisión de las infracciones tipificadas en los artículos 38.3 c), d) e i) y 38.4 d), g) y h) de esta Ley.

2. La potestad sancionadora regulada en esta Ley se ejercerá de conformidad con lo establecido al respecto en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y en sus normas de desarrollo. El procedimiento tendrá una duración máxima de nueve meses a contar desde la fecha del acuerdo de iniciación. El plazo máximo de duración del procedimiento simplificado será de tres meses.

Artículo 44. *Concurrencia de infracciones y sanciones.*

1. No podrá ejercerse la potestad sancionadora a que se refiere la presente Ley cuando haya recaído sanción penal, en los casos en que se aprecie identidad de sujeto, hecho y fundamento.

No obstante, cuando se esté tramitando un proceso penal por los mismos hechos o por otros cuya separación de los sancionables con arreglo a esta Ley sea racionalmente imposible, el procedimiento quedará suspendido respecto de los mismos hasta que recaiga pronunciamiento firme de la autoridad judicial.

Reanudado el expediente, en su caso, la resolución que se dicte deberá respetar los hechos declarados probados en la resolución judicial.

2. La imposición de una sanción prevista en esta Ley no impedirá la tramitación y resolución de otro procedimiento sancionador por los órganos u organismos competentes en cada caso cuando la conducta infractora se hubiera cometido utilizando técnicas y medios telemáticos o electrónicos y resulte tipificada en otra Ley, siempre que no haya identidad del bien jurídico protegido.

3. No procederá la imposición de sanciones según lo previsto en esta Ley cuando los hechos constitutivos de infracción lo sean también de otra tipificada en la normativa sectorial a la que esté sujeto el prestador del servicio y exista identidad del bien jurídico protegido.

Cuando, como consecuencia de una actuación sancionadora, se tuviera conocimiento de hechos que pudieran ser constitutivos de infracciones tipificadas en otras leyes, se dará cuenta de los mismos a los órganos u organismos competentes para su supervisión y sanción.

Artículo 45. *Prescripción.*

Las infracciones muy graves prescribirán a los tres años, las graves a los dos años y las leves a los seis meses; las sanciones impuestas por faltas muy graves prescribirán a los tres años, las impuestas por faltas graves a los dos años y las impuestas por faltas leves al año.

Disposición adicional primera. *Significado de los términos empleados por esta Ley.*

A los efectos de la presente Ley, los términos definidos en el anexo tendrán el significado que allí se les asigna.

Disposición adicional segunda. *Medicamentos y productos sanitarios.*

La prestación de servicios de la sociedad de la información relacionados con los medicamentos y los productos sanitarios se regirá por lo dispuesto en su legislación específica.

Disposición adicional tercera. *Sistema Arbitral de Consumo.*

El prestador y el destinatario de servicios de la sociedad de la información podrán someter sus conflictos al arbitraje de consumo, mediante la adhesión de aquéllos al Sistema Arbitral de Consumo competente que se prestará también por medios electrónicos, conforme al procedimiento establecido reglamentariamente.

Disposición adicional cuarta. *Modificación de los Códigos Civil y de Comercio.*

Uno. Se modifica el artículo 1.262 del Código Civil, que queda redactado de la siguiente manera:

> «El consentimiento se manifiesta por el concurso de la oferta y de la aceptación sobre la cosa y la causa que han de constituir el contrato.
>
> Hallándose en lugares distintos el que hizo la oferta y el que la aceptó, hay consentimiento desde que el oferente conoce la aceptación o desde que, habiéndosela remitido el aceptante, no pueda ignorarla sin faltar a la buena fe. El contrato, en tal caso, se presume celebrado en el lugar en que se hizo la oferta.
>
> En los contratos celebrados mediante dispositivos automáticos hay consentimiento desde que se manifiesta la aceptación.»

Dos. Se modifica el artículo 54 del Código de Comercio, que queda redactado de la siguiente manera:

> «Hallándose en lugares distintos el que hizo la oferta y el que la aceptó, hay consentimiento desde que el oferente conoce la aceptación o desde que,

habiéndosela remitido el aceptante, no pueda ignorarla sin faltar a la buena fe. El contrato, en tal caso, se presume celebrado en el lugar en que se hizo la oferta.

En los contratos celebrados mediante dispositivos automáticos hay consentimiento desde que se manifiesta la aceptación.»

Disposición adicional quinta. *Accesibilidad para las personas con discapacidad y de edad avanzada a la información proporcionada por medios electrónicos.*

(Derogada)

Disposición adicional sexta. *Sistema de asignación de nombres de dominio bajo el ".es".*

Uno. Esta disposición regula, en cumplimiento de lo previsto en la disposición adicional decimosexta de la Ley 17/2001, de 7 de diciembre, de Marcas, los principios inspiradores del sistema de asignación de nombres de dominio bajo el código de país correspondiente a España ".es".

Dos. La entidad pública empresarial Red.es es la autoridad de asignación, a la que corresponde la gestión del registro de nombres de dominio de Internet bajo el ".es", de acuerdo con lo establecido en la disposición adicional sexta de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones.

Tres. La asignación de nombres de dominio de Internet bajo el ".es" se realizará de conformidad con los criterios que se establecen en esta disposición, en el Plan Nacional de Nombres de Dominio de Internet, en las demás normas específicas que se dicten en su desarrollo por la autoridad de asignación y, en la medida en que sean compatibles con ellos, con las prácticas generalmente aplicadas y las recomendaciones emanadas de las entidades y organismos internacionales que desarrollan actividades relacionadas con la gestión del sistema de nombres de dominio de Internet.

Los criterios de asignación de nombres de dominio bajo el ".es" deberán garantizar un equilibrio adecuado entre la confianza y seguridad jurídica precisas para el desarrollo del comercio electrónico y de otros servicios y actividades por vía electrónica, y la flexibilidad y agilidad requeridas para posibilitar la satisfacción de la demanda de asignación de nombres de dominio bajo el ".es", contribuyendo, de esta manera, al desarrollo de la sociedad de la información en España.

Podrán crearse espacios diferenciados bajo el ".es", que faciliten la identificación de los contenidos que alberguen en función de su titular o del tipo de actividad que realicen. Entre otros, podrán crearse indicativos relacionados con la educación, el entretenimiento y el adecuado desarrollo moral de la infancia y juventud. Estos nombres de dominio de tercer nivel se asignarán en los términos que se establezcan en el Plan Nacional de Nombres de Dominio de Internet.

Cuatro. Podrán solicitar la asignación de nombres de dominio bajo el ".es", en los términos que se prevean en el Plan Nacional de Nombres de Dominio de Internet, todas las personas o entidades, con o sin personalidad jurídica, que tengan intereses o mantengan vínculos con España, siempre que reúnan los demás requisitos exigibles para la obtención de un nombre de dominio.

Los nombres de dominio bajo el ".es" se asignarán al primer solicitante que tenga derecho a ello, sin que pueda otorgarse, con carácter general, un derecho preferente para la obtención o utilización de un nombre de dominio a los titulares de determinados derechos.

La asignación de un nombre de dominio confiere a su titular el derecho a su utilización, el cual estará condicionado al cumplimiento de los requisitos que en cada caso se establezcan, así como a su mantenimiento en el tiempo. La verificación por parte de la autoridad de asignación del incumplimiento de estos requisitos dará lugar a la cancelación del nombre de dominio, previa la tramitación del procedimiento que en cada caso se determine y que deberá garantizar la audiencia de los interesados.

Los beneficiarios de un nombre de dominio bajo el ".es" deberán respetar las reglas y condiciones técnicas que pueda establecer la autoridad de asignación para el adecuado funcionamiento del sistema de nombres de dominio bajo el ".es".

La responsabilidad del uso correcto de un nombre de dominio de acuerdo con las leyes, así como del respeto a los derechos de propiedad intelectual o industrial, corresponde a la persona u organización para la que se haya registrado dicho nombre de dominio, en los

términos previstos en esta Ley. La autoridad de asignación procederá a la cancelación de aquellos nombres de dominio cuyos titulares infrinjan esos derechos o condiciones, siempre que así se ordene en la correspondiente resolución judicial, sin perjuicio de lo que se prevea en aplicación del apartado ocho de esta disposición adicional.

Cinco. En el Plan Nacional de Nombres de Dominio de Internet se establecerán mecanismos apropiados para prevenir el registro abusivo o especulativo de nombres de dominio, el aprovechamiento indebido de términos de significado genérico o topónimos y, en general, para prevenir los conflictos que se puedan derivar de la asignación de nombres de dominio.

Asimismo, el Plan incluirá las cautelas necesarias para minimizar el riesgo de error o confusión de los usuarios en cuanto a la titularidad de nombres de dominio.

A estos efectos, la entidad pública empresarial Red.es establecerá la necesaria coordinación con los registros públicos españoles. Sus titulares deberán facilitar el acceso y consulta a dichos registros públicos, que, en todo caso, tendrá carácter gratuito para la entidad.

Cinco bis. La autoridad de asignación suspenderá cautelarmente o cancelará, de acuerdo con el correspondiente requerimiento judicial previo, los nombres de dominio mediante los cuales se esté cometiendo un delito o falta tipificado en el Código Penal. Del mismo modo procederá la autoridad de asignación cuando por las Fuerzas y Cuerpos de Seguridad del Estado se le dirija requerimiento de suspensión cautelar dictado como diligencia de prevención dentro de las 24 horas siguientes al conocimiento de los hechos.

Asimismo, de acuerdo con lo dispuesto en los artículos 8, 11 y concordantes de esta Ley, la autoridad administrativa o judicial competente como medida para obtener la interrupción de la prestación de un servicio de la sociedad de la información o la retirada de un contenido, podrá requerir a la autoridad de asignación para que suspenda cautelarmente o cancele un nombre de dominio.

De la misma forma se procederá en los demás supuestos previstos legalmente.

En los supuestos previstos en los dos párrafos anteriores, sólo podrá ordenarse la suspensión cautelar o la cancelación de un nombre de dominio cuando el prestador de servicios o persona responsable no hubiera atendido el requerimiento dictado para el cese de la actividad ilícita.

En todos los casos en que la Constitución, las normas reguladoras de los respectivos derechos y libertades o las que resulten aplicables a las diferentes materias atribuyan competencia a los órganos jurisdiccionales de forma excluyente para intervenir en el ejercicio de actividades o derechos, sólo la autoridad judicial competente podrá requerir la suspensión cautelar o la cancelación. En particular, cuando dichas medidas afecten a los derechos y libertades de expresión e información y demás amparados en los términos establecidos en el artículo 20 de la Constitución solo podrán ser decididas por los órganos jurisdiccionales competentes.

La suspensión consistirá en la imposibilidad de utilizar el nombre de dominio a los efectos del direccionamiento en Internet y la prohibición de modificar la titularidad y los datos registrales del mismo, si bien podrá añadir nuevos datos de contacto. El titular del nombre de dominio únicamente podrá renovar el mismo o modificar la modalidad de renovación. La suspensión cautelar se mantendrá hasta que sea levantada o bien, confirmada en una resolución definitiva que ordene la cancelación del nombre de dominio.

La cancelación tendrá los mismos efectos que la suspensión hasta la expiración del período de registro y si el tiempo restante es inferior a un año, por un año adicional, transcurrido el cual el nombre de dominio podrá volver a asignarse.

Seis. La asignación de nombres de dominio se llevará a cabo por medios telemáticos que garanticen la agilidad y fiabilidad de los procedimientos de registro.

La presentación de solicitudes y la práctica de notificaciones se realizarán por vía electrónica, salvo en los supuestos en que así esté previsto en los procedimientos de asignación y demás operaciones asociadas al registro de nombres de dominio.

Los agentes registradores, como intermediarios en los procedimientos relacionados con el registro de nombres de dominio, podrán prestar servicios auxiliares para la asignación y renovación de éstos, de acuerdo con los requisitos y condiciones que determine la autoridad

de asignación, los cuales garantizarán, en todo caso, el respeto al principio de libre competencia entre dichos agentes.

Siete. El Plan Nacional de Nombres de Dominio de Internet se aprobará mediante Orden del Ministro de Ciencia y Tecnología, a propuesta de la entidad pública empresarial Red.es.

El Plan se completará con los procedimientos para la asignación y demás operaciones asociadas al registro de nombres de dominio y direcciones de Internet que establezca el Presidente de la entidad pública empresarial Red.es, de acuerdo con lo previsto en la disposición adicional decimoctava de la Ley 14/2000, de 29 de diciembre, de Medidas fiscales, administrativas y del orden social.

Ocho. En los términos que permitan las disposiciones aplicables, la autoridad de asignación podrá establecer un sistema de resolución extrajudicial de conflictos sobre la utilización de nombres de dominio, incluidos los relacionados con los derechos de propiedad industrial. Este sistema, que asegurará a las partes afectadas las garantías procesales adecuadas, se aplicará sin perjuicio de las eventuales acciones judiciales que las partes puedan ejercitar.

Nueve. Con la finalidad de impulsar el desarrollo de la Administración electrónica, la entidad pública empresarial Red.es podrá prestar el servicio de notificaciones administrativas telemáticas y acreditar de forma fehaciente la fecha y hora de su recepción.

Disposición adicional séptima. *Fomento de la Sociedad de la Información.*

El Ministerio de Ciencia y Tecnología como Departamento de la Administración General del Estado responsable de la propuesta al Gobierno y de la ejecución de las políticas tendentes a promover el desarrollo en España de la Sociedad de la Información, la generación de valor añadido nacional y la consolidación de una industria nacional sólida y eficiente de productos, servicios y contenidos de la Sociedad de la Información, presentará al Gobierno para su aprobación y a las Cortes Generales un plan cuatrienal para el desarrollo de la Sociedad de la Información y de convergencia con Europa con objetivos mensurables, estructurado en torno a acciones concretas, con mecanismos de seguimiento efectivos, que aborde de forma equilibrada todos los frentes de actuación, contemplando diversos horizontes de maduración de las iniciativas y asegurando la cooperación y la coordinación del conjunto de las Administraciones públicas.

Este plan establecerá, asimismo, los objetivos, las acciones, los recursos y la periodificación del proceso de convergencia con los países de nuestro entorno comunitario en línea con las decisiones y recomendaciones de la Unión Europea.

En este sentido, el plan deberá:

Potenciar decididamente las iniciativas de formación y educación en las tecnologías de la información para extender su uso; especialmente, en el ámbito de la educación, la cultura, la gestión de las empresas, el comercio electrónico y la sanidad.

Profundizar en la implantación del gobierno y la administración electrónica incrementando el nivel de participación ciudadana y mejorando el grado de eficiencia de las Administraciones públicas.

Disposición adicional octava. *Colaboración de los registros de nombres de dominio establecidos en España en la lucha contra actividades ilícitas.*

1. Los registros de nombres de dominio establecidos en España estarán sujetos a lo establecido en el apartado Cinco bis de la disposición adicional sexta, respecto de los nombres de dominio que asignen.

2. Las entidades de registro de nombres de dominio establecidas en España estarán obligadas a facilitar los datos relativos a los titulares de los nombres de dominio que soliciten las autoridades públicas para el ejercicio de sus competencias de inspección, control y sanción cuando las infracciones administrativas que se persigan tengan relación directa con la actividad de una página de Internet identificada con los nombres de dominio que asignen.

Tales datos se facilitarán así mismo, cuando sean necesarios para la investigación y mitigación de incidentes de ciberseguridad en los que estén involucrados equipos relacionados con un nombre de dominio de los encomendados a su gestión. Dicha

información será proporcionada al órgano, organismo o entidad que se determine legal o reglamentariamente.

En ambos supuestos, la solicitud deberá formularse mediante escrito motivado en el que se especificarán los datos requeridos y la necesidad y proporcionalidad de los datos solicitados para el fin que se persigue. Si los datos demandados son datos personales, su cesión no precisará el consentimiento de su titular.

Disposición adicional novena. *Gestión de incidentes de ciberseguridad que afecten a la red de Internet.*

1. Los prestadores de servicios de la Sociedad de la Información, los registros de nombres de dominio y los agentes registradores que estén establecidos en España están obligados a prestar su colaboración con el CERT competente, en la resolución de incidentes de ciberseguridad que afecten a la red de Internet y actuar bajo las recomendaciones de seguridad indicadas o que sean establecidas en los códigos de conducta que de esta Ley se deriven.

Los órganos, organismos públicos o cualquier otra entidad del sector público que gestionen equipos de respuesta a incidentes de seguridad colaborarán con las autoridades competentes para la aportación de las evidencias técnicas necesarias para la persecución de los delitos derivados de dichos incidentes de ciberseguridad.

2. Para el ejercicio de las funciones y obligaciones anteriores, los prestadores de servicios de la Sociedad de la información, respetando el secreto de las comunicaciones, suministrarán la información necesaria al CERT competente, y a las autoridades competentes, para la adecuada gestión de los incidentes de ciberseguridad, incluyendo las direcciones IP que puedan hallarse comprometidas o implicadas en los mismos.

De la misma forma, los órganos, organismos públicos o cualquier otra entidad del sector público que gestionen equipos de respuesta a incidentes de seguridad podrán intercambiar información asociada a incidentes de ciberseguridad con otros CERTs o autoridades competentes a nivel nacional e internacional, siempre que dicha información sea necesaria para la prevención de incidentes en su ámbito de actuación.

3. El Gobierno pondrá en marcha, en el plazo de seis meses, un programa para impulsar un esquema de cooperación público-privada con el fin de identificar y mitigar los ataques e incidentes de ciberseguridad que afecten a la red de Internet en España. Para ello, se elaborarán códigos de conducta en materia de ciberseguridad aplicables a los diferentes prestadores de servicios de la sociedad de la información, y a los registros de nombres de dominio y agentes registradores establecidos en España.

Los códigos de conducta determinarán el conjunto de normas, medidas y recomendaciones a implementar que permitan garantizar una gestión eficiente y eficaz de dichos incidentes de ciberseguridad, el régimen de colaboración y condiciones de adhesión e implementación, así como los procedimientos de análisis y revisión de las iniciativas resultantes.

La Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información coordinará las actuaciones que se pongan en marcha derivadas de estos códigos de conducta.

4. Conforme a los códigos de conducta que se definan en particular, los prestadores de servicios de la sociedad de la información deberán identificar a los usuarios afectados por los incidentes de ciberseguridad que les sean notificados por el CERT competente, e indicarles las acciones que deben llevar a cabo y que están bajo su responsabilidad, así como los tiempos de actuación. En todo caso, se les proporcionará información sobre los perjuicios que podrían sufrir u ocasionar a terceros si no colaboran en la resolución de los incidentes de ciberseguridad a que se refiere esta disposición.

En el caso de que los usuarios no ejerciesen en el plazo recomendado su responsabilidad en cuanto a la desinfección o eliminación de los elementos causantes del incidente de ciberseguridad, los prestadores de servicios deberán, bajo requerimiento del CERT competente, aislar dicho equipo o servicio de la red, evitando así efectos negativos a terceros hasta el cese de la actividad maliciosa.

El párrafo anterior será de aplicación a cualquier equipo o servicio geolocalizado en España o que esté operativo bajo un nombre de dominio «.es» u otros cuyo Registro esté establecido en España.

5. Reglamentariamente se determinará los órganos, organismos públicos o cualquier otra entidad del sector público que ejercerán las funciones de equipo de respuesta a incidentes de seguridad o CERT competente a los efectos de lo previsto en la presente disposición.

6. La Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información garantizará un intercambio fluido de información con la Secretaría de Estado de Seguridad del Ministerio del Interior sobre incidentes, amenazas y vulnerabilidades según lo contemplado en la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la Protección de las Infraestructuras Críticas. En este sentido se establecerán mecanismos de coordinación entre ambos órganos para garantizar la provisión de una respuesta coordinada frente a incidentes en el marco de la presente Ley.

Disposición transitoria única. *Anotación en los correspondientes registros públicos de los nombres de dominio otorgados antes de la entrada en vigor de esta Ley.*

Los prestadores de servicios que, a la entrada en vigor de esta Ley, ya vinieran utilizando uno o más nombres de dominio o direcciones de Internet deberán solicitar la anotación de, al menos, uno de ellos en el registro público en que figuraran inscritos a efectos constitutivos o de publicidad, en el plazo de un año desde la referida entrada en vigor.

Disposición final primera. *Modificación del artículo 37 de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones.*

Se modifica el párrafo a) del apartado 1 del artículo 37 de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, que queda redactada en los siguientes términos:

> «a) Que los ciudadanos puedan recibir conexión a la red telefónica pública fija y acceder a la prestación del servicio telefónico fijo disponible para el público. La conexión debe ofrecer al usuario la posibilidad de emitir y recibir llamadas nacionales e internacionales y permitir la transmisión de voz, fax y datos a velocidad suficiente para acceder de forma funcional a Internet.
>
> A estos efectos, se considerará que la velocidad suficiente a la que se refiere el párrafo anterior es la que se utiliza de manera generalizada para acceder a Internet por los abonados al servicio telefónico fijo disponible para el público con conexión a la red mediante pares de cobre y módem para banda vocal.»

Disposición final segunda. *Modificación de la disposición adicional sexta de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones.*

Se modifica el apartado 10 de la disposición adicional sexta de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, que quedará redactado como sigue:

> «10. Tasa por asignación del recurso limitado de nombres de dominio y direcciones de Internet.
>
> a) Hecho imponible.
>
> El hecho imponible de la tasa por asignación de nombres de dominio y direcciones de Internet estará constituido por la realización por la entidad pública empresarial Red.es de las actividades necesarias para la asignación y renovación de nombres de dominio y direcciones de Internet bajo el código de país correspondiente a España (.es).
>
> b) Sujetos pasivos.
>
> Serán sujetos pasivos de la tasa los solicitantes de la asignación o renovación de los nombres y direcciones de Internet.
>
> c) Cuantía.
>
> La cuantía de la tasa será única por cada nombre o dirección cuya asignación o renovación se solicite. En ningún caso se procederá a la asignación o a la renovación del nombre o dirección sin que se haya efectuado previamente el pago de la tasa.

Sólo podrán modificarse mediante Ley el número e identidad de los elementos y criterios de cuantificación con base en los cuales se determinan las cuotas exigibles.

A los efectos previstos en el párrafo anterior, se consideran elementos y criterios de cuantificación del importe exigible por asignación anual inicial de los nombres de dominio o direcciones de Internet el número asignado, el coste de las actividades de comprobación y verificación de las solicitudes de asignación, así como el nivel en que se produzca la asignación y, en el caso de renovación anual en los años sucesivos, el coste del mantenimiento de la asignación y de las actividades de comprobación y de actualización de datos.

Igualmente, se atenderá al número de nombres o direcciones de Internet asignados y a la actuación a través de agentes registradores para concretar la cuantía de la tasa.

El establecimiento y modificación de las cuantías resultantes de la aplicación de los elementos y criterios de cuantificación a que se refieren los párrafos anteriores podrá efectuarse mediante Orden ministerial.

No obstante lo dispuesto en los párrafos anteriores de este apartado, en los supuestos de carácter excepcional en que así esté previsto en el Plan Nacional de Nombres de Dominio de Internet y en los términos que en el mismo se fijen, con base en el especial valor de mercado del uso de determinados nombres y direcciones, la cuantía por asignación anual inicial podrá sustituirse por la que resulte de un procedimiento de licitación en el que se fijará un valor inicial de referencia estimado. Si el valor de adjudicación de la licitación resultase superior a dicho valor de referencia, aquél constituirá el importe de la tasa. En los supuestos en que se siga este procedimiento de licitación, el Ministerio de Ciencia y Tecnología requerirá, con carácter previo a su convocatoria, a la autoridad competente para el Registro de Nombres de Dominio para que suspenda el otorgamiento de los nombres y direcciones que considere afectados por su especial valor económico. A continuación, se procederá a aprobar el correspondiente pliego de bases que establecerá, tomando en consideración lo previsto en el Plan Nacional de Nombres de Dominio de Internet, los requisitos, condiciones y régimen aplicable a la licitación.

d) Devengo.

La tasa se devengará en la fecha en que se proceda, en los términos que se establezcan reglamentariamente, a la admisión de la solicitud de asignación o de renovación de los nombres o direcciones de Internet, que no se tramitará sin que se haya efectuado el pago correspondiente.

e) Exacción y gestión recaudatoria.

La exacción de la tasa se producirá a partir de la atribución de su gestión a la entidad pública empresarial Red.es y de la determinación del procedimiento para su liquidación y pago, mediante Orden ministerial.

Los modelos de declaración, plazos y formas de pago de la tasa se aprobarán mediante resolución de la entidad pública empresarial Red.es.

El importe de los ingresos obtenidos por esta tasa se destinará a financiar los gastos de la entidad pública empresarial Red.es por las actividades realizadas en el cumplimiento de las funciones asignadas a la misma en los párrafos a), b), c) y d) del apartado 4 de esta disposición, ingresándose, en su caso, el excedente en el Tesoro Público, de acuerdo con la proporción y cuantía que se determine mediante resolución conjunta de las Secretarías de Estado de Presupuestos y Gastos y de Telecomunicaciones y para la Sociedad de la Información, a propuesta de esta última.»

Disposición final tercera. *Adición de una nueva disposición transitoria a la Ley 11/1998, de 24 de abril, General de Telecomunicaciones.*

Se añade a la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, una nueva disposición transitoria duodécima, con la siguiente redacción:

«Disposición transitoria duodécima. *Criterios para el desarrollo del plan de actualización tecnológica de la red de acceso de la red telefónica pública fija.*

En el plazo máximo de cinco meses a partir de la entrada en vigor de esta disposición, el operador designado para la prestación del servicio universal presentará al Ministerio de Ciencia y Tecnología, para su aprobación en el plazo de un mes, previo informe de la Comisión del Mercado de las Telecomunicaciones, un plan de actuación detallado para garantizar que las conexiones a la red telefónica pública fija posibiliten a sus abonados el acceso funcional a Internet y, en particular, a los conectados mediante Telefonía Rural de Acceso Celular (TRAC).

El desarrollo del plan estará sujeto a las siguientes condiciones:

a) Incluirá soluciones tecnológicas eficientes disponibles en el mercado para garantizar el derecho de los usuarios a disponer, previa solicitud a partir de la aprobación del plan, de la posibilidad de acceso funcional a Internet en el plazo máximo de sesenta días desde la fecha de dicha solicitud en las zonas con cobertura. Estas soluciones tecnológicas deberán prever su evolución a medio plazo hacia velocidades de banda ancha sin que ello conlleve necesariamente su sustitución.

b) La implantación en la red de acceso de las soluciones tecnológicas a las que se refiere el párrafo a) deberá alcanzar a los abonados al servicio telefónico fijo disponible al público que, en la fecha de aprobación del plan, no tienen la posibilidad de acceso funcional a Internet, de acuerdo con el siguiente calendario:

1.º Al menos al 30 por 100 antes del 30 de junio de 2003.
2.º Al menos al 70 por 100 antes del 31 de diciembre de 2003.
3.º El 100 por 100 antes del 31 de diciembre de 2004.

En todo caso, esta implantación alcanzará, al menos, al 50 por 100 de los citados abonados en cada una de las Comunidades Autónomas antes del 31 de diciembre de 2003.

c) En el plan de actuación deberá priorizarse el despliegue al que se refiere el párrafo b) con arreglo al criterio de mayor densidad de abonados afectados.

d) A los efectos de lo dispuesto en los apartados anteriores y en caso de que sea necesario, el operador designado para la prestación del servicio universal podrá concluir con otros operadores titulares de concesiones de dominio público radioeléctrico, contratos de cesión de derechos de uso de las bandas de frecuencias necesarias para el cumplimiento de los objetivos establecidos en esta disposición. Dichos contratos deberán ser sometidos a la previa aprobación por parte del Ministerio de Ciencia y Tecnología, que podrá establecer las condiciones de salvaguarda del interés público que estime necesarias.»

Disposición final cuarta. *Modificación de la disposición derogatoria única de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones.*

Se modifica el último párrafo de la disposición derogatoria única de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, que queda redactado de la siguiente forma:

«Igualmente, quedan derogadas cuantas otras disposiciones de igual o inferior rango a la presente Ley se opongan a lo dispuesto en ella y, en especial, a lo dispuesto en el artículo 37.1.ª), en lo relativo a la velocidad de transmisión de datos.»

Disposición final quinta. *Adecuación de la regulación reglamentaria sobre contratación telefónica o electrónica con condiciones generales a esta Ley.*

El Gobierno, en el plazo de un año, modificará el Real Decreto 1906/1999, de 17 de diciembre, por el que se regula la contratación telefónica o electrónica con condiciones generales en desarrollo del artículo 5.3 de la Ley 7/1998, de 13 de abril, sobre condiciones generales de la contratación, para adaptar su contenido a lo dispuesto en esta Ley.

En dicha modificación, el Gobierno tendrá especialmente en cuenta la necesidad de facilitar la utilización real de los contratos electrónicos, conforme al mandato recogido en el artículo 9.1 de la Directiva 2000/31/CE.

Disposición final sexta. *Fundamento constitucional.*

Esta Ley se dicta al amparo del artículo 149.1.6.ª, 8.ª y 21.ª de la Constitución, sin perjuicio de las competencias de las Comunidades Autónomas.

Disposición final séptima. *Habilitación al Gobierno.*

Se habilita al Gobierno para desarrollar mediante Reglamento lo previsto en esta Ley.

Disposición final octava. *Distintivo de adhesión a códigos de conducta que incorporen determinadas garantías.*

En el plazo de un año a partir de la entrada en vigor de esta Ley, el Gobierno aprobará un distintivo que permita identificar a los prestadores de servicios que respeten códigos de conducta adoptados con la participación del Consejo de Consumidores y Usuarios, y que incluyan, entre otros contenidos, la adhesión al Sistema Arbitral de Consumo o a otros sistemas de resolución extrajudicial de conflictos que respeten los principios establecidos en la normativa comunitaria sobre sistemas alternativos de resolución de conflictos con consumidores, en los términos que reglamentariamente se establezcan.

Disposición final novena. *Entrada en vigor.*

Esta Ley entrará en vigor a los tres meses de su publicación en el "Boletín Oficial del Estado".

No obstante, las disposiciones adicional sexta y finales primera, segunda, tercera y cuarta de esta Ley entrarán en vigor el día siguiente al de su publicación en el "Boletín Oficial del Estado".

ANEXO

Definiciones

A los efectos de esta Ley, se entenderá por:

a) "Servicios de la sociedad de la información" o "servicios": todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario.

El concepto de servicio de la sociedad de la información comprende también los servicios no remunerados por sus destinatarios, en la medida en que constituyan una actividad económica para el prestador de servicios.

Son servicios de la sociedad de la información, entre otros y siempre que representen una actividad económica, los siguientes:

1.º La contratación de bienes o servicios por vía electrónica.

2.º La organización y gestión de subastas por medios electrónicos o de mercados y centros comerciales virtuales.

3.º La gestión de compras en la red por grupos de personas.

4.º El envío de comunicaciones comerciales.

5.º El suministro de información por vía telemática.

No tendrán la consideración de servicios de la sociedad de la información los que no reúnan las características señaladas en el primer párrafo de este apartado y, en particular, los siguientes:

1.º Los servicios prestados por medio de telefonía vocal, fax o télex.

2.º El intercambio de información por medio de correo electrónico u otro medio de comunicación electrónica equivalente para fines ajenos a la actividad económica de quienes lo utilizan.

3.º Los servicios de radiodifusión televisiva (incluidos los servicios de cuasivídeo a la carta), contemplados en el artículo 3.ª) de la Ley 25/1994, de 12 de julio, por la que se incorpora al ordenamiento jurídico español la Directiva 89/552/CEE, del Consejo, de 3 de octubre, sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas al ejercicio de actividades de radiodifusión televisiva, o cualquier otra que la sustituya.

4.º Los servicios de radiodifusión sonora, y

5.º El teletexto televisivo y otros servicios equivalentes como las guías electrónicas de programas ofrecidas a través de las plataformas televisivas.

b) "Servicio de intermediación": servicio de la sociedad de la información por el que se facilita la prestación o utilización de otros servicios de la sociedad de la información o el acceso a la información.

Son servicios de intermediación la provisión de servicios de acceso a Internet, la transmisión de datos por redes de telecomunicaciones, la realización de copia temporal de las páginas de Internet solicitadas por los usuarios, el alojamiento en los propios servidores de datos, aplicaciones o servicios suministrados por otros y la provisión de instrumentos de búsqueda, acceso y recopilación de datos o de enlaces a otros sitios de Internet.

c) "Prestador de servicios" o "prestador": persona física o jurídica que proporciona un servicio de la sociedad de la información.

d) "Destinatario del servicio" o "destinatario": persona física o jurídica que utiliza, sea o no por motivos profesionales, un servicio de la sociedad de la información.

e) "Consumidor": persona física o jurídica en los términos establecidos en el artículo 1 de la Ley 26/1984, de 19 de julio, General para la Defensa de los Consumidores y Usuarios.

f) "Comunicación comercial": toda forma de comunicación dirigida a la promoción, directa o indirecta, de la imagen o de los bienes o servicios de una empresa, organización o persona que realice una actividad comercial, industrial, artesanal o profesional.

A efectos de esta Ley, no tendrán la consideración de comunicación comercial los datos que permitan acceder directamente a la actividad de una persona, empresa u organización, tales como el nombre de dominio o la dirección de correo electrónico, ni las comunicaciones relativas a los bienes, los servicios o la imagen que se ofrezca cuando sean elaboradas por un tercero y sin contraprestación económica.

g) "Profesión regulada": toda actividad profesional que requiera para su ejercicio la obtención de un título, en virtud de disposiciones legales o reglamentarias.

h) "Contrato celebrado por vía electrónica" o "contrato electrónico": todo contrato en el que la oferta y la aceptación se transmiten por medio de equipos electrónicos de tratamiento y almacenamiento de datos, conectados a una red de telecomunicaciones.

i) "Ámbito normativo coordinado": todos los requisitos aplicables a los prestadores de servicios de la sociedad de la información, ya vengan exigidos por la presente Ley u otras normas que regulen el ejercicio de actividades económicas por vía electrónica, o por las leyes generales que les sean de aplicación, y que se refieran a los siguientes aspectos:

1.º Comienzo de la actividad, como las titulaciones profesionales o cualificaciones requeridas, la publicidad registral, las autorizaciones administrativas o colegiales precisas, los regímenes de notificación a cualquier órgano u organismo público o privado, y

2.º Posterior ejercicio de dicha actividad, como los requisitos referentes a la actuación del prestador de servicios, a la calidad, seguridad y contenido del servicio, o los que afectan a la publicidad y a la contratación por vía electrónica y a la responsabilidad del prestador de servicios.

No quedan incluidos en este ámbito las condiciones relativas a las mercancías y bienes tangibles, a su entrega ni a los servicios no prestados por medios electrónicos.

j) "Órgano competente": todo órgano jurisdiccional o administrativo, ya sea de la Administración General del Estado, de las Administraciones Autonómicas, de las Entidades locales o de sus respectivos organismos o entes públicos dependientes, que actúe en el ejercicio de competencias legalmente atribuidas.

§ 34

Real Decreto 381/2015, de 14 de mayo, por el que se establecen medidas contra el tráfico no permitido y el tráfico irregular con fines fraudulentos en comunicaciones electrónicas

Ministerio de Industria, Energía y Turismo
«BOE» núm. 127, de 28 de mayo de 2015
Última modificación: sin modificaciones
Referencia: BOE-A-2015-5854

En el ámbito de los servicios de comunicaciones electrónicas existen agentes que desarrollan actividades destinadas a obtener un lucro económico indebido, que van desde simples usos oportunistas de las ofertas comerciales de los operadores, pasando por acciones que conllevan infracciones administrativas, hasta otras que implican actividades ilícitas, tanto relacionadas con los propios servicios de telecomunicaciones como con otros servicios conexos, como la comercialización de contenidos o los terminales y equipamientos de usuario.

Estas actividades pueden adoptar diferentes formas, que evolucionan con el tiempo, siendo las más habituales las que se aprovechan de la cadena de pagos por servicios o contenidos soportados por redes de telecomunicaciones que implican la concesión de crédito por un operador a un tercero, ya sea otro operador o un usuario final, que con frecuencia resulta impagado.

Así, estas comunicaciones suelen caracterizarse por ser generadas y prolongadas de manera artificial con el fin de obtener un lucro de la cadena de pagos de facturación. Inicialmente estas prácticas se asociaban a servicios de tarificación elevada, que ofrecen mayores márgenes de beneficio, extendiéndose sin embargo en la actualidad a todo tipo de servicios y numeraciones mediante técnicas de generación de llamadas masivas, aumentando el perjuicio económico a los operadores y usuarios y pudiendo llegar a generar problemas de calidad de servicio, e incluso poner en riesgo la seguridad y la integridad de las redes y servicios a causa de la elevada ocupación de recursos provocada.

Además, cuando estas prácticas conllevan usos no permitidos de recursos públicos de numeración, no solo constituyen una infracción de la normativa nacional específica que puede abordarse mediante un adecuado control del uso de la numeración, sino que pueden llegar a comprometer acuerdos internacionales suscritos tanto por los operadores como por el propio Reino de España cuando se realiza un uso indebido de numeración internacional.

La Comisión del Mercado de las Telecomunicaciones, organismo actualmente integrado en la Comisión Nacional de los Mercados y la Competencia, aprobó distintas resoluciones para autorizar de manera individual a los operadores para proceder al bloqueo del tráfico en determinados supuestos, así como una resolución, de 5 de septiembre de 2013, por la que se aprueba un procedimiento común para la suspensión de la interconexión de numeraciones por tráfico irregular.

El artículo 51 de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones establece en su apartado segundo que, mediante real decreto, se establecerán las condiciones en las que los operadores de redes públicas de comunicaciones electrónicas o servicios de comunicaciones electrónicas disponibles al público lleven a cabo el bloqueo de acceso a números o servicios siempre que esté justificado por motivos de tráfico no permitido y de tráfico irregular con fines fraudulentos, y los casos en que los prestadores de servicios de comunicaciones electrónicas retengan los correspondientes ingresos por interconexión u otros servicios.

Por su parte, el artículo 19 de dicha Ley establece los principios generales de la numeración, direccionamiento y denominación de los servicios de comunicaciones electrónicas.

Por todo ello, resulta necesario adoptar medidas normativas contra el tráfico no permitido y el tráfico irregular con fines fraudulentos, encaminadas tanto a eliminar los incentivos para estas prácticas como a asegurar el correcto uso de los recursos públicos de numeración, al tiempo que se garantiza la calidad de los servicios de comunicaciones electrónicas y, muy especialmente, la integridad y la seguridad de redes y servicios de comunicaciones electrónicas.

A los efectos del presente real decreto, existen dos tipos de tráfico no permitido, por un lado, el tráfico no permitido que usa numeración no autorizada y, por otro lado, el tráfico no permitido que hace un uso indebido de la numeración.

Se considera tráfico no permitido que usa numeración no autorizada el que tenga origen o destino en recursos públicos de numeración que no hayan sido atribuidos, habilitados o asignados conforme a los correspondientes planes nacionales e internacionales de numeración. Este tipo de tráfico, que se puede identificar por sus características técnicas, deberá ser bloqueado por los operadores tan pronto tengan constancia del mismo.

A su vez, el tráfico no permitido que hace un uso indebido de la numeración es aquel que, empleando numeración que sí está atribuida o habilitada y asignada, responde a usos indebidos de dicha numeración, si bien tal circunstancia no puede establecerse a priori sino tras un análisis caso por caso de sus circunstancias específicas.

Por último, se encuentra el tráfico irregular con fines fraudulentos, que es el generado, inducido o prolongado artificialmente, así como provocado a través de comunicaciones comerciales no solicitadas o mediante el control no consentido de los sistemas o terminales de usuario, al objeto de hacer un uso abusivo o fraudulento de las redes y los servicios, lo que igualmente solo puede determinarse tras un análisis caso por caso de las características específicas del tráfico.

Para todos los tipos de tráfico no permitido y tráfico irregular señalados, se establece que los operadores deben ser capaces de identificar la existencia de esta clase de tráfico en las redes que operen y en los servicios que presten, como paso previo e indispensable para llevar a cabo las debidas actuaciones contra estos tráficos, en particular cuando así les sea requerido por la Administración.

Los operadores deberán bloquear la transmisión hacia otros operadores o proveedores del tráfico no permitido que usa numeración no autorizada tan pronto como lo identifiquen, quedando obligados a identificar al menos dicho tráfico cuando es generado en sus redes y con destino en recursos de numeración pertenecientes a los planes nacionales.

Para los supuestos de tráfico no permitido que hace un uso indebido de la numeración y tráfico irregular con fines fraudulentos, se articulan actuaciones escalonadas que se inician con una solicitud del operador afectado a la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información para que verifique si existe un tráfico no permitido que hace un uso indebido de la numeración o un tráfico irregular con fines fraudulentos, y autorice al bloqueo de estas comunicaciones.

Con el fin de agilizar la toma de medidas por parte de los operadores, se prevé la autorización de criterios para la puesta en funcionamiento de procedimientos específicos para que los operadores, tras una evaluación caso por caso, puedan retener los pagos relacionados con estos tráficos, así como para que puedan bloquear el tráfico dirigido a numeraciones individuales.

Tanto para el supuesto de tráfico no permitido que hace un uso indebido de la numeración como para el de tráfico irregular con fines fraudulentos, se considera la

posibilidad de que las actuaciones iniciadas por el operador tengan su origen en un conflicto entre operadores en materia de acceso o interconexión, correspondiendo en tales casos a la Comisión Nacional de los Mercados y la Competencia resolver sobre los mismos en virtud de sus competencias en la materia.

De otro lado, se prevé la posibilidad de que la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información pueda adoptar medidas cautelares y requerir a los operadores para que adopten las medidas pertinentes, con el fin de garantizar la integridad y seguridad de las redes y servicios de comunicaciones electrónicas, la calidad en la prestación de servicios de comunicaciones electrónicas, o los derechos específicos de los usuarios de telecomunicaciones, entre otros objetivos, para lo que los operadores deben ser capaces de identificar el tráfico no permitido y el tráfico irregular en las redes que operen y en los servicios que presten.

Por otra parte, se prevé la adaptación de los acuerdos de acceso e interconexión entre operadores al objeto de que incorporen las disposiciones necesarias para la aplicación del presente real decreto, explicitando que la falta de adecuación de los acuerdos no exime del cumplimiento de lo establecido en el mismo, cuyas disposiciones serán efectivas desde el momento de su entrada en vigor.

Por último, se contempla que los operadores que tuvieran implantados procedimientos o sistemas previamente aprobados por la Comisión del Mercado de las Telecomunicaciones o por la Comisión Nacional de los Mercados y la Competencia para la suspensión de la interconexión de numeraciones por tráfico irregular, puedan seguir utilizándolos durante un mes tras la entrada en vigor del presente real decreto, si bien los operadores que soliciten la autorización de criterios para la implantación de sistemas o procedimientos según lo establecido en este real decreto podrán seguir utilizando dichos procedimientos previamente aprobados hasta que la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información resuelva sobre esta solicitud.

Las medidas contenidas en el presente real decreto se dictan de conformidad con los artículos 19 y 20, y con el apartado 2 del artículo 51 de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

Este real decreto se dicta al amparo de la competencia exclusiva del Estado en materia de telecomunicaciones, reconocida en el artículo 149.1.21.ª de la Constitución.

En su virtud, a propuesta del Ministro de Industria, Energía y Turismo, con la aprobación previa del Ministro de Hacienda y Administraciones Públicas y de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros en su reunión del día 14 de mayo de 2015,

DISPONGO:

Artículo 1. *Objeto y ámbito de aplicación.*

1. El presente real decreto establece medidas y actuaciones destinadas a prevenir y evitar el tráfico que tenga origen o destino en recursos públicos de numeración que no hayan sido atribuidos, habilitados o asignados; determinados tipos de tráfico contrarios a lo establecido en las disposiciones de atribución, habilitación o asignación de recursos nacionales e internacionales de numeración; así como el tráfico irregular con fines fraudulentos cursado en las redes públicas y servicios de comunicaciones electrónicas disponibles al público.

2. El presente real decreto se aplica a los operadores que exploten redes públicas de comunicaciones electrónicas o presten servicios de comunicaciones electrónicas disponibles al público.

3. Los objetivos del presente real decreto son proteger la integridad de las redes y la seguridad de las redes y servicios de comunicaciones electrónicas, asegurar la calidad en la prestación de los servicios de comunicaciones electrónicas y garantizar los derechos de los usuarios. Asimismo, se persigue reducir los perjuicios económicos sufridos tanto por los operadores como por los usuarios.

Artículo 2. *Concepto de tráfico no permitido.*

1. A los efectos del presente real decreto, existen dos tipos de tráfico no permitido:

a) Tráfico no permitido que usa numeración no autorizada.
b) Tráfico no permitido que hace un uso indebido de la numeración.

2. Se considera tráfico no permitido que usa numeración no autorizada el que tenga origen o destino en recursos públicos de numeración que no hayan sido atribuidos, habilitados o asignados, pertenecientes a los siguientes planes e instrucciones sobre recursos de numeración:

a) El plan nacional de numeración telefónica, aprobado mediante Real Decreto 2296/2004, de 10 de diciembre,
b) las instrucciones sobre la utilización de recursos públicos de numeración para la prestación de servicios de mensajes cortos de texto y mensajes multimedia, establecidas en la Orden ITC/308/2008, de 31 de enero,
c) el plan internacional de numeración descrito en la recomendación E.164 del Sector de Normalización de las Telecomunicaciones de la Unión Internacional de Telecomunicaciones (UIT-T), incluyendo en este último caso los códigos de país o de red internacional que no hayan sido atribuidos por el UIT-T, los rangos de numeración que no hayan sido comunicados por las correspondientes autoridades nacionales a través del boletín de explotación del UIT-T, y los destinos identificados por procedimientos de marcación contrarios a lo recogido en la correspondiente lista anexa del citado boletín.
d) Cualquier otro plan de numeración que se determine por orden del Ministerio de Industria, Energía y Turismo.

3. Se considera tráfico no permitido que hace un uso indebido de la numeración el que tenga origen o destino en recursos públicos de numeración de los planes identificados en el apartado anterior que hayan sido asignados y que haga un uso de dichos recursos contrario a las condiciones de uso establecidas en las correspondientes disposiciones de atribución, habilitación o aplicación.

Artículo 3. *Concepto de tráfico irregular con fines fraudulentos.*

1. A los efectos del presente real decreto, se considera tráfico irregular el que presenta características que difieren significativamente de los patrones habituales de tráfico cursado bajo un funcionamiento ordinario de la red o de los servicios correspondiente a prácticas comerciales generalmente aceptadas en la prestación de los servicios de comunicaciones electrónicas, en aspectos tales como su volumen, número de conexiones o distribución en el tiempo, para determinados orígenes, destinos, rutas o áreas geográficas.
2. El tráfico irregular tendrá fines fraudulentos cuando resulte generado, inducido o prolongado artificialmente al objeto de obtener lucro, directo o indirecto, de la cadena de facturación de pagos en la prestación de servicios de comunicaciones electrónicas disponibles al público.
En particular tendrá dicha consideración el que, cumpliendo las condiciones anteriores, responda, entre otros, a los siguientes supuestos:

a) El basado en el agotamiento de los saldos o límites de crédito de determinados usuarios mediante comunicaciones dirigidas a rutas o destinos determinados,
b) el basado en la utilización abusiva de bonos, tarifas planas o esquemas de tarificación similares dirigidos a usuarios finales para la generación de tráfico ficticio o mediante su puesta a disposición de terceros en condiciones contrarias a lo previsto en los contratos,
c) el provocado o inducido por comunicaciones no solicitadas, o
d) el provocado mediante la manipulación o control no consentido de los sistemas o terminales de usuario.

Artículo 4. *Identificación de tráfico no permitido y tráfico irregular con fines fraudulentos.*

1. Todos los operadores deberán ser capaces de identificar el tráfico no permitido que usa numeración no autorizada, cuando tenga origen en sus redes y destino en recursos públicos de numeración a los que se refieren los apartados a), b) o d) del artículo 2.2.

2. Los operadores podrán implantar procedimientos y sistemas que, basándose en las características del tráfico, permitan identificar los tipos de tráficos que obedezcan a los conceptos recogidos en los artículos 2 y 3, y actuar sobre ellos, en particular reteniendo los correspondientes pagos de interconexión, acceso o interoperabilidad, o bloqueando la transmisión de determinados tipos de tráfico, según lo dispuesto en los artículos siguientes.

3. Mediante orden del Ministerio de Industria, Energía y Turismo se podrán establecer requisitos que deban ser satisfechos por tales procedimientos y sistemas y, en su caso, la obligatoriedad de que sean sometidos a una auditoría periódica por una entidad externa, así como los requisitos que deberán cumplir las entidades auditoras y los criterios para la realización de las auditorías.

4. Los operadores que pretendan implantar tales sistemas o procedimientos lo notificarán a la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información detallando los criterios empleados para identificar los diferentes tipos de tráfico, y pondrán a su disposición toda la información sobre sus características y operativa, que deberán estar debidamente documentados y desarrollados para permitir tanto su inspección por los servicios pertinentes de la Administración, como su auditoría por una entidad externa.

5. En el plazo máximo de tres meses desde la recepción de la notificación a la que se refiere el apartado anterior, la Secretaria de Estado de Telecomunicaciones y para la Sociedad de la Información dictará resolución motivada, autorizando o denegando la utilización de los criterios notificados. Dicha autorización constituye requisito previo para la puesta en funcionamiento de los citados procedimientos y sistemas.

Transcurrido el plazo al que se refiere al párrafo anterior sin que haya recaído resolución expresa, deberá entenderse desestimada la solicitud, sin perjuicio de la obligación de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información de resolver expresamente.

Contra las resoluciones, que agotan la vía administrativa, se podrá interponer recurso potestativo de reposición ante el mismo órgano que la haya dictado en el plazo de un mes desde el día siguiente a su notificación, de acuerdo con los artículos 116 y 117 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, o bien ser impugnadas directamente ante el órgano competente del orden jurisdiccional de lo contencioso-administrativo en el plazo de dos meses contados desde el día siguiente a la notificación, sin que puedan ser simultáneos ambos recursos.

Asimismo, con posterioridad a la puesta en funcionamiento, la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información podrá dictar instrucciones vinculantes relativas a estos sistemas o procedimientos, destinadas a garantizar el cumplimiento efectivo de lo dispuesto en el presente real decreto o en sus disposiciones de desarrollo.

Artículo 5. *Actuaciones ante el tráfico no permitido que usa numeración no autorizada.*

Los operadores que identifiquen en sus redes o servicios tráfico no permitido que usa numeración no autorizada deberán bloquear su transmisión hacia otros operadores o proveedores, y lo notificarán a la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, así como a los operadores y proveedores de servicios a los que afecte este bloqueo con los que mantengan una relación contractual.

Estas notificaciones deberán realizarse en un plazo máximo de dos días hábiles a contar desde el momento de la identificación del tráfico no permitido que usa numeración no autorizada por parte del operador. En la notificación dirigida a la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, se deberá indicar el momento de la identificación del tráfico no permitido que usa numeración no autorizada así como, en su caso, información que acredite el momento en que dicho tráfico comenzó a producirse, si ambos hechos no fueron simultáneos.

Artículo 6. *Actuaciones ante el tráfico no permitido que hace un uso indebido de la numeración o el tráfico irregular con fines fraudulentos.*

1. Los operadores que identifiquen en sus redes o servicios tráfico que consideren que pueda responder al supuesto de tráfico no permitido que hace un uso indebido de la numeración o de tráfico irregular con fines fraudulentos podrán presentar una solicitud

razonada requiriendo autorización para el bloqueo provisional de la transmisión de dicho tráfico, dirigida a la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, bien en cualquiera de los lugares que se mencionan en el artículo 38.4 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, bien a través de la sede electrónica del Ministerio de Industria, Energía y Turismo.

En dicha solicitud, el operador deberá aportar las razones así como toda la información de que disponga que justifique que el tráfico afectado debe considerarse como tráfico no permitido que hace un uso indebido de la numeración o como tráfico irregular con fines fraudulentos, incluyendo la indicación del momento de su identificación por parte del operador así como, en su caso, información que acredite el momento en que dicho tráfico comenzó a producirse, si ambos hechos no fueron simultáneos.

La Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información resolverá dichas solicitudes y notificará la resolución adoptada en un plazo máximo de tres meses, autorizando o denegando el bloqueo de la transmisión del tráfico, pudiendo a tal efecto recabar informe a la Comisión Nacional de los Mercados y la Competencia sobre el impacto del bloqueo solicitado en la regulación ex ante de los mercados, y podrá adoptar medidas cautelares autorizando al bloqueo de la transmisión del tráfico.

Transcurrido el plazo al que se refiere al párrafo anterior sin que haya recaído resolución expresa, deberá entenderse desestimada la solicitud, sin perjuicio de la obligación de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información de resolver expresamente.

Contra las resoluciones, que agotan la vía administrativa, se podrá interponer recurso potestativo de reposición ante el mismo órgano que la haya dictado en el plazo de un mes desde el día siguiente a su notificación, de acuerdo con los artículos 116 y 117 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, o bien ser impugnadas directamente ante el órgano competente del orden jurisdiccional de lo contencioso-administrativo en el plazo de dos meses contados desde el día siguiente a la notificación, sin que puedan ser simultáneos ambos recursos.

2. Alternativamente a lo establecido en el apartado anterior, los operadores que identifiquen tráfico no permitido que hace un uso indebido de la numeración o tráfico irregular con fines fraudulentos mediante los procedimientos o sistemas a los que se refiere el artículo 4 podrán, tras una evaluación caso por caso, retener los pagos correspondientes al mismo, aplicando la retención desde el momento de la identificación de dicho tráfico o, en el caso de que el momento de la identificación sea posterior al de la producción, desde el momento en que acrediten que el tráfico comenzó a producirse, con un plazo de treinta días naturales anteriores a la fecha de identificación, salvo que en sus acuerdos de interconexión, acceso e interoperabilidad acuerden un plazo distinto.

Asimismo, dichos operadores, tras una evaluación caso por caso, podrán bloquear temporalmente el tráfico dirigido a numeraciones individuales que correspondan a determinados orígenes, destinos o relaciones contractuales, de conformidad con los criterios autorizados por la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, según lo establecido en el artículo 4.

El operador que realice retención de pagos o bloqueo de tráfico será responsable frente a las posibles reclamaciones de los titulares de la numeración afectada por los posibles perjuicios causados por dicho bloqueo.

Cuando los operadores realicen retención de pagos o bloqueo de transmisión de tráfico según lo establecido en este apartado, lo notificarán a los operadores y proveedores de servicios a los que afecte este tráfico con los que mantengan una relación contractual, así como a la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información aportando en este último caso toda la información necesaria para identificar el tráfico afectado, los criterios utilizados en su evaluación y las medidas concretas adoptadas. Estas notificaciones deberán realizarse en un plazo máximo de dos días hábiles a contar desde el momento de la identificación del tráfico por el operador. En todo momento el operador podrá aportar información complementaria o adicional que permita identificar con mayor precisión el tráfico afectado.

En el plazo máximo de tres meses a contar desde el momento en que se reciba la notificación de retención de pagos o bloqueo de transmisión de tráfico a que se refiere este apartado, la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información podrá incoar un expediente para supervisar las medidas adoptadas por el operador, a raíz del cual podrá ordenar el cese del bloqueo de la transmisión del tráfico y, en su caso, la realización del pago de las cantidades que hubiesen sido retenidas, incrementadas con el interés legal del dinero. Asimismo, la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información podrá adoptar medidas cautelares requiriendo al operador que no proceda a la retención de pagos, al bloqueo de la transmisión del tráfico o a ambas medidas simultáneamente.

3. Los operadores deberán aportar toda la información complementaria que les sea requerida por la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información en relación con los eventos de identificación de tráfico no permitido que hace un uso indebido de la numeración o de tráfico irregular con fines fraudulentos, o de las correspondientes medidas adoptadas, ya sea como complemento a la información que hayan remitido en las notificaciones realizadas de acuerdo con el presente artículo o en relación con notificaciones realizadas por otros operadores.

La Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información podrá establecer el contenido y formato en que deban presentarse las notificaciones y la información complementaria requerida.

4. Si de la tramitación de los expedientes a los que se refieren los apartados anteriores se desprende que las solicitudes o notificaciones correspondientes tienen su origen en un conflicto entre operadores en materia de acceso o interconexión, la Comisión Nacional de los Mercados y la Competencia resolverá sobre los extremos objeto del conflicto, de acuerdo con lo señalado en el artículo 15 de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

Artículo 7. *Medidas y actuaciones por requerimiento de la Administración.*

La Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información podrá en todo momento, de oficio, conforme a los trámites procedimentales y plazos establecidos en el artículo 6.1, requerir a los operadores la aplicación de medidas de bloqueo de la transmisión de tráfico, de retención de pagos o ambas simultáneamente en relación con el tráfico no permitido o el tráfico irregular, y, en su caso, adoptar medidas cautelares, con los objetivos de:

a) Garantizar la integridad de las redes y la seguridad de las redes y servicios de comunicaciones electrónicas.

b) Garantizar la calidad en la prestación de los servicios de comunicaciones electrónicas.

c) Garantizar los derechos específicos de los usuarios de telecomunicaciones.

d) Controlar el uso de la numeración asignada, en particular para garantizar el cumplimiento de las condiciones ligadas al uso de los recursos públicos de numeración establecidas en los planes e instrucciones referidos en el artículo 2.

e) Garantizar el cumplimiento de compromisos en materia de telecomunicaciones asumidos por el Reino de España en organismos internacionales, en particular en relación con el cumplimiento de las condiciones ligadas al uso de los recursos públicos de numeración internacional descritos en la recomendación E.164 de la Unión Internacional de Telecomunicaciones.

Los operadores deberán ser capaces de identificar en las redes que operen y en los servicios que presten, el tráfico al que se refieran las citadas medidas para garantizar su cumplimiento efectivo.

Disposición adicional primera. *Duración máxima de los bloqueos de tráfico.*

Los operadores que bloqueen tráfico de acuerdo con lo establecido en el artículo 6 podrán mantener dicho bloqueo durante un período máximo de doce meses, salvo que la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información resuelva estableciendo la aplicación de un plazo distinto. Transcurrido este plazo, los operadores no podrán aplicar el bloqueo. Por orden del Ministerio de Industria, Energía y Turismo podrá

fijarse una duración máxima distinta, que podrá ser diferente en función del tipo de tráfico de que se trate.

Asimismo, los operadores no podrán aplicar el bloqueo si se produce un cambio en la titularidad del abonado de las numeraciones individuales afectadas y así se lo solicita el operador asignatario de las mismas, así como cuando dichas numeraciones se asignen a otro operador.

Disposición adicional segunda. *Acuerdos de interconexión, acceso e interoperabilidad.*

1. Los acuerdos de interconexión, acceso e interoperabilidad entre operadores celebrados de conformidad con lo establecido en la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones y en el Reglamento sobre mercados de comunicaciones electrónicas, acceso a las redes y numeración, aprobado por Real Decreto 2296/2004, de 10 de diciembre, se adecuarán a lo establecido en el presente real decreto y en sus disposiciones de desarrollo.

En particular, dichos acuerdos deberán describir los procedimientos que se aplicarán para el bloqueo del tráfico, la retención de los pagos y las correspondientes notificaciones al resto de operadores o proveedores de servicios.

Mediante orden del Ministerio de Industria, Energía y Turismo se podrán establecer los requisitos que han de contemplar dichos acuerdos cuando, para asegurar el cumplimiento de lo establecido en el presente real decreto, sea necesaria la colaboración entre operadores con relaciones contractuales mayoristas.

La falta de adecuación de los acuerdos no exime del cumplimiento de lo establecido en el presente real decreto, cuyas disposiciones serán efectivas desde el momento de su entrada en vigor.

2. La Comisión Nacional de los Mercados y la Competencia entenderá de los conflictos entre operadores en la negociación de estos acuerdos.

Disposición adicional tercera. *Limitación del gasto.*

Las medidas incluidas en esta norma no podrán suponer incremento de dotaciones ni de retribuciones ni de otros gastos de personal.

Disposición transitoria primera. *Modificación de los acuerdos de interconexión, acceso e interoperabilidad entre operadores.*

En el plazo de cuatro meses desde la entrada en vigor del presente real decreto, los operadores a los que se refiere el artículo 1 revisarán y en su caso modificarán los acuerdos de interconexión, acceso a redes y a sus recursos asociados e interoperabilidad de servicios, de acuerdo con lo establecido en la disposición adicional segunda.

Disposición transitoria segunda. *Procedimientos aprobados previamente por la Administración.*

Los operadores que tuvieran implantados procedimientos previamente aprobados por la Comisión del Mercado de las Telecomunicaciones o por la Comisión Nacional de los Mercados y la Competencia para la suspensión de la interconexión de numeraciones por tráfico irregular, podrán seguir utilizando dichos procedimientos ante la Comisión Nacional de los Mercados y la Competencia en las mismas condiciones en las que lo venían haciendo durante un mes tras la entrada en vigor del presente real decreto.

No obstante, los operadores que soliciten la autorización de criterios para la implantación de sistemas o procedimientos según lo establecido en el artículo 4 del presente real decreto en el plazo de un mes a contar desde su entrada en vigor, podrán seguir utilizando dichos procedimientos previamente aprobados hasta que la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información resuelva sobre esta solicitud.

Disposición final primera. *Título competencial.*

Este real decreto se dicta al amparo de la competencia exclusiva del Estado en materia de telecomunicaciones reconocida en el artículo 149.1.21.ª de la Constitución.

Disposición final segunda. *Desarrollo reglamentario y aplicación.*

El Ministro de Industria, Energía y Turismo dictará, en el ámbito de sus competencias, cuantas disposiciones y medidas sean necesarias para el desarrollo y aplicación de lo establecido en el este real decreto.

Disposición final tercera. *Entrada en vigor.*

El presente real decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

§ 35

Orden TDF/149/2025, de 12 de febrero, por la que se establecen medidas para combatir las estafas de suplantación de identidad a través de llamadas telefónicas y mensajes de texto fraudulentos y para garantizar la identificación de la numeración utilizada para la prestación de servicios de atención al cliente y realización de llamadas comerciales no solicitadas

Ministerio para la Transformación Digital y de la Función Pública
«BOE» núm. 40, de 15 de febrero de 2025
Última modificación: sin modificaciones
Referencia: BOE-A-2025-2870

En los últimos años estamos asistiendo a un incremento exponencial de la cibercriminalidad y, en particular, de las estafas de suplantación de identidad que suelen comenzar con una llamada o un mensaje de texto en los que el emisor de la comunicación suplanta la identidad de una organización de confianza (entidad bancaria, administración pública, empresa de transporte, etc.) con la clara intención de defraudar, engañando al consumidor para que proporcione información personal y financiera confidencial, facilite sus claves personales o realice alguna acción como el acceso a una web, la llamada a un número telefónico, la realización de una trasferencia, o la contratación de un servicio, entre otros.

La confianza de los consumidores en la fiabilidad y seguridad del contenido transmitido a través de las redes, el amplio uso que hacen las empresas y organismos de las comunicaciones electrónicas como medio para contactar con sus usuarios, así como la capacidad de estas comunicaciones para llegar a un gran número de personas a un coste relativamente bajo, hacen que el uso de llamadas y mensajes de texto sea un instrumento frecuentemente utilizado en la comisión de este tipo de estafas.

Estas estafas causan importantes daños financieros y económicos a todos los sectores de la sociedad, incluidos los consumidores, las empresas y los organismos públicos. Además, disminuyen la confianza de los consumidores en las comunicaciones electrónicas, provocando que, a raíz de la generalización de estas prácticas, desconfíen de contestar llamadas y leer mensajes de texto, perjudicando a aquellas empresas y organismos que hacen un uso legítimo de llamadas y mensajes de texto, como canal de comunicación para facilitar información u ofrecer sus servicios a los consumidores.

Por ello con el objetivo, recogido en el artículo 3 de la Ley 11/2022, de 28 de junio, General de Telecomunicaciones, de defender los intereses de los usuarios, restaurando la confianza de los consumidores en las comunicaciones electrónicas, entre los días 14 de febrero y 8 de marzo de 2024, se han sometido a consulta pública una serie de opciones técnicas y regulatorias destinadas a prevenir y combatir este tipo de estafas y prácticas fraudulentas que se canalizan a través de llamadas y mensajes de texto.

De las respuestas a dicha consulta pública se concluye la necesidad de adoptar medidas en distintos ámbitos.

De acuerdo con ello, la presente norma adopta soluciones para evitar que progresen las comunicaciones con manipulación del identificador de línea llamante (CLI, por sus siglas en inglés), introduce mecanismos para evitar fraudes en el ámbito de la numeración y los códigos alfanuméricos identificativos de mensajes cortos y establece medidas para garantizar la correcta identificación de la numeración utilizada para la prestación del servicio de atención a clientes o para la realización de llamadas comerciales no solicitadas.

El capítulo I de disposiciones generales establece el objeto y ámbito de aplicación de la norma y define los términos utilizados en la misma.

Dentro del capítulo II, el artículo 4 desarrolla lo establecido en el artículo 2.2.a) del Real Decreto 381/2015, de 14 de mayo, por el que se establecen medidas contra el tráfico no permitido y el tráfico irregular con fines fraudulentos en comunicaciones electrónicas, obligando a los operadores a bloquear aquellas llamadas que presenten el campo del CLI vacío o que presenten como CLI numeración perteneciente al plan nacional de numeración telefónica, que no haya sido atribuida, asignada o adjudicada.

En muchas de las aportaciones recibidas se destaca, asimismo, que en numerosas ocasiones las estafas canalizadas a través de llamadas utilizan la manipulación del CLI, para que el número coincida con el número publicitado (o conocido por los usuarios) de una entidad financiera, empresa prestadora de otros servicios o de un organismo público, cuya trazabilidad se dificulta por la participación de estafadores que están localizados fuera del territorio nacional.

De acuerdo con ello, el artículo 5, en desarrollo del citado artículo 2.2.a) del Real Decreto 381/2015, de 14 de mayo, conforme a lo establecido en el artículo 81 del Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, aprobado por Real Decreto 424/2005, de 15 de abril y en el artículo 30 del Reglamento sobre mercados de comunicaciones electrónicas, acceso a las redes y numeración, aprobado por Real Decreto 2296/2004, de 10 de diciembre obliga a los operadores a bloquear las llamadas con origen internacional identificadas por un CLI del plan nacional de numeración, salvo que se trate de un caso de itinerancia internacional.

Asimismo, para atajar estas prácticas en el ámbito de la mensajería móvil, en el capítulo III, de acuerdo con el citado artículo 30 del Reglamento sobre mercados de comunicaciones electrónicas, acceso a las redes y numeración, se añade a las obligaciones ya previstas en la Orden ITC/308/2008, de 31 de enero, por la que se dictan instrucciones sobre la utilización de recursos públicos de numeración para la prestación de servicios de mensajes cortos de texto y mensajes multimedia, la obligación de los operadores que proporcionen servicios de comunicaciones electrónicas de almacenamiento y reenvío de mensajes, de bloquear los mensajes que usan numeración que no haya sido atribuida, asignada o adjudicada, incluyendo numeración vacía, así como aquellos mensajes con origen internacional que estén identificados por un CLI del plan nacional de numeración, salvo en los casos de itinerancia internacional.

En este capítulo III se obliga, asimismo, a los operadores a bloquear todos aquellos SMS/MMS/RCS que hagan uso de caracteres alfanuméricos (alias) que no consten en el Registro gestionado al efecto por la Comisión Nacional de los Mercados y de la Competencia o que hayan sido emitidos por proveedores de servicios de mensajería que no hayan sido habilitados en dicho registro para el envío y transmisión de SMS/MMS/RCS utilizando como identificador el alias inscrito.

Por último, en el capítulo IV, se adoptan medidas para garantizar la correcta identificación de la numeración utilizada para la prestación de servicios de atención a clientes o para la realización de llamadas comerciales no solicitadas, que en todo caso deberán garantizar los derechos de los usuarios conforme a lo establecido en el artículo 66.1.b) de la Ley 11/2022, de 28 de junio, General de Telecomunicaciones.

En primer lugar, para permitir una mejor identificación de estas llamadas, en desarrollo del artículo 27.7 del Reglamento sobre mercados de comunicaciones electrónicas, acceso a las redes y numeración, aprobado por Real Decreto 2296/2004, de 10 de diciembre, se prohíbe usar para estas llamadas numeración móvil, lo que obliga, asimismo, a revisar la

redacción de la Resolución de 27 de mayo de 2013, por la que se modifica la atribución de los rangos de numeración para comunicaciones móviles.

En segundo lugar, conforme al artículo 61.2 del Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, se permite, con carácter general, la utilización de numeración 800 y 900 para la realización de estas llamadas, de modo que, devolver las llamadas a estos números, resulte gratuito para los consumidores.

La norma se adecua a los principios de buena regulación previstos en el artículo 129 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. En particular la norma se ajusta a los principios de necesidad y eficacia, al estar justificada por razones de interés general en defensa de los intereses de los usuarios. La norma se adecua asimismo al principio de proporcionalidad, al contener la regulación imprescindible para atender las necesidades que pretende cubrir. En cuanto al principio de eficiencia, la norma evita cargas administrativas innecesarias o accesorias y racionaliza, en su aplicación, la gestión de los recursos públicos. La norma responde al principio de seguridad jurídica, puesto que desarrolla normativa ya aprobada, siendo su adopción predecible ante el considerable aumento de este tipo de prácticas. Por último, la norma responde al principio de transparencia, toda vez que ha sido objeto de consulta y audiencia y será objeto de publicación en el «Boletín Oficial del Estado».

En cumplimiento de lo previsto en la Ley 50/1997, de 27 de noviembre, del Gobierno, esta disposición ha sido sometida al preceptivo trámite de consulta pública y de audiencia e información pública.

Durante la tramitación de la norma, se ha recabado el informe preceptivo de la Comisión Nacional de los Mercados y la Competencia de conformidad con el artículo 5.2.a) de la Ley 3/2013, de 4 de junio, de creación de la Comisión Nacional de los Mercados y la Competencia y el artículo 100.2.x) de la Ley 11/2022, de 28 de julio, General de Telecomunicaciones.

Asimismo, se ha recabado informe preceptivo del Consejo de Consumidores y Usuarios, en virtud del artículo 39 del texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, aprobado por el Real Decreto Legislativo 1/2007, de 16 de noviembre, y en el artículo 2.a) del Real Decreto 894/2005, de 22 de julio, por el que se regula el Consejo de Consumidores y Usuarios.

La presente norma se dicta al amparo de lo previsto en el artículo 3 de la Ley 11/2022, de 28 de junio, General de Telecomunicaciones, en el artículo 2.2.a) del Real Decreto 381/2015, de 14 de mayo, en los artículos 27.7 y 30 del Reglamento sobre mercados de comunicaciones electrónicas, acceso a las redes y numeración y en los artículos 61.2 y 81 del Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios.

En su virtud, dispongo:

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

1. La presente orden tiene por objeto la adopción de medidas para evitar que progresen las comunicaciones con manipulación del identificador de línea llamante o CLI.

2. La presente orden introduce mecanismos para evitar fraudes en el ámbito de la numeración y de los alias identificativos de mensajes cortos, mensajes multimedia y servicios de mensajería conversacional (SMS/MMS/RCS).

3. Asimismo, la presente orden establece medidas para garantizar la correcta identificación de la numeración utilizada para la prestación del servicio de atención a clientes o para la realización de llamadas comerciales no solicitadas.

Artículo 2. *Ámbito de aplicación.*

1. Las obligaciones establecidas en los capítulos II y III de la presente orden se aplican a los operadores que presten servicios de comunicaciones interpersonales, los prestadores de

almacenamiento y reenvío de mensajes y sus respectivos revendedores en la medida en que permitan establecer comunicaciones (llamadas y mensajes) mediante el empleo de números del Plan Nacional de Numeración Telefónica, o de la Orden ITC/308/2008, de 31 de enero, por la que se dictan instrucciones sobre la utilización de recursos públicos de numeración para la prestación de servicios de mensajes cortos de texto y mensajes multimedia, o alias.

2. En el caso del artículo 4 resultará obligado al bloqueo el operador que origina la llamada. En el caso del artículo 5, resultará obligado al bloqueo el operador que recibe la llamada por una interfaz internacional de interconexión. El resto de operadores que transiten o terminen la llamada podrán realizar el bloqueo en los supuestos recogidos en dichos artículos.

3. Las obligaciones establecidas en el capítulo IV de la presente orden aplican a los prestadores de servicios de atención al cliente o a quienes realizan llamadas comerciales no solicitadas.

Artículo 3. *Definiciones.*

A los efectos de esta orden se entiende por:

a) Alias: cadena de caracteres alfanumérica transmitida en el campo destinado al CLI en las comunicaciones a través de SMS/MMS/RCS, que informa del remitente, pero no es un recurso público susceptible de devolver el mensaje.

b) Número de teléfono español: número de teléfono incluido en el plan nacional de numeración telefónica para el servicio de telefonía fija o móvil. Incluye la numeración geográfica del servicio telefónico fijo, y la numeración geográfica y no geográfica del servicio nómada, así como aquellos otros números pertenecientes a rangos de numeración 800/900 y numeración corta, cuyo uso haya sido autorizado por la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales como identificador de la línea llamante.

c) Identificador de línea llamante o CLI: número del plan nacional de numeración telefónica perteneciente al abonado del que procede la llamada o cuyo uso haya sido autorizado por la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales. En la señalización SIP *(Session Initiation Protocol)*, este identificador se encuentra en el campo PAI *(P-Asserted-Identity)* y también puede encontrarse en el campo *From*, independientemente de si la llamada ha sido previamente desviada o no. En la señalización ISUP *(ISDN User Part)* el parámetro equivalente sería *Calling Party Number.*

d) Número de teléfono llamado: número de teléfono perteneciente al abonado al que se dirige la llamada.

e) Interfaz internacional de interconexión: punto en el que una llamada internacional llega a España por una interfaz que pertenece a un proveedor de servicios de comunicaciones electrónicas inscrito en el Registro de Operadores gestionado por la Comisión Nacional de los Mercados y la Competencia.

f) Itinerancia internacional: el uso por un cliente itinerante de un dispositivo móvil para efectuar o recibir llamadas, o para enviar o recibir mensajes SMS/MMS/RCS o para usar comunicaciones de datos por conmutación de paquetes, cuando se encuentra en un país distinto, en virtud de acuerdos celebrados entre el operador de la red de origen y el operador de la red visitada.

g) Servicio de comunicaciones vocales: un servicio de comunicaciones electrónicas disponible para el público a través de uno o más números de un plan nacional o internacional de numeración telefónica, para efectuar y recibir, directa o indirectamente, llamadas nacionales e internacionales.

CAPÍTULO II

Medidas para evitar que progresen las comunicaciones con manipulación del identificador de línea llamante

Artículo 4. *Bloqueo del tráfico que usa numeración que no haya sido atribuida, asignada o adjudicada, incluyendo numeración vacía.*

1. Los operadores deberán bloquear las llamadas de servicios de comunicación vocal con CLI vacío o que presenten como CLI un número de teléfono español que no esté atribuido a ningún servicio o cuyo formato no sea coherente con el plan nacional de numeración telefónica, aprobado mediante Real Decreto 2296/2004, de 10 de diciembre, por el que se aprueba el Reglamento sobre mercados de comunicaciones electrónicas, acceso a las redes y numeración y sus disposiciones de desarrollo, el plan internacional de numeración descrito en la recomendación E.164 del Sector de Normalización de las Telecomunicaciones de la Unión Internacional de Telecomunicaciones (UIT-T), y cualquier otro plan de numeración que se determine por orden del Ministerio para la Transformación Digital y de la Función Pública.

2. Los operadores deberán bloquear las llamadas de servicios de comunicación vocal que presenten como CLI numeraciones que no hayan sido asignadas por la Comisión Nacional de los Mercados y la Competencia a ningún operador o proveedor de servicios de comunicaciones electrónicas, para lo que deberán consultar la correspondiente base de datos gestionada por dicha comisión.

3. Asimismo, cada operador deberá bloquear las llamadas de servicios de comunicación vocal que presenten como CLI numeraciones que le hayan sido asignadas, subasignadas o portadas y que ese operador todavía no haya adjudicado a ningún cliente.

La Comisión Nacional de los Mercados y la Competencia establecerá el mecanismo para aquellos casos en los que un operador tenga revendedores en su red a quienes les haya subasignado numeración, sin que se produzca un intercambio de información comercial entre competidores.

4. Las llamadas recibidas por un operador, actuando este operador en terminación o tránsito, que presenten un CLI que el propio operador tenga asignado o portado deberán ser bloqueadas, salvo que se trate de un caso de itinerancia internacional, en cuyo caso se aplicará lo establecido en el artículo 5.2.

5. Este artículo se aplica independientemente de si la llamada se realiza dentro de España o entra en España desde el extranjero a través de una interfaz internacional de interconexión.

6. Por resolución de la persona titular de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales podrá exceptuarse de la obligación de bloqueo determinados supuestos debidamente justificados.

Las excepciones se notificarán a la Comisión Nacional de los Mercados y la Competencia, y se publicarán en el portal de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales.

Artículo 5. *Bloqueo de llamadas con origen internacional identificadas por un CLI del plan nacional de numeración fija o móvil.*

1. Deberán bloquearse las llamadas de servicios de comunicación vocal, recibidas desde el extranjero cuando presenten como CLI un número de teléfono español, salvo que se trate de un caso de itinerancia internacional.

2. La comprobación de si se trata de un caso de itinerancia internacional deberá llevarse a cabo por el operador a través de los instrumentos, mecanismos y procedimientos que tenga implementados a tal fin.

En los casos en que no resulte técnicamente viable conocer si se trata de un caso de itinerancia internacional, el operador podrá aplicar los criterios destinados a identificar casos de tráfico irregular con fines fraudulentos que se aprueben por resolución de la persona titular de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales.

Asimismo, en los casos en que no resulte técnicamente viable conocer si se trata de un caso de itinerancia internacional, antes de entregar la llamada al destinatario, el operador

podrá introducir una marca para evitar la presentación del CLI o un parámetro de señalización que indique que el CLI no ha sido verificado. Atendiendo a la evolución tecnológica, a la existencia de distintos parámetros e instrumentos técnicos para identificar cuando se esté en un supuesto de itinerancia internacional, a las pautas de tráfico y consumo y al volumen de llamadas en las que no pueda conocerse si existe itinerancia internacional, mediante resolución de la persona titular de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales podrá establecerse una fecha a partir de la cual la introducción de las citadas marcas o parámetros de señalización resultará obligatoria.

3. Por resolución de la persona titular de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales podrá exceptuarse de la obligación de bloqueo determinados supuestos debidamente justificados, así como aquellos escenarios en los que se permita que no coincidan el campo PAI y el campo *From* del CLI.

Las excepciones se notificarán a la Comisión Nacional de los Mercados y la Competencia, y se publicarán en el portal de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales.

4. Las llamadas telefónicas internacionales sólo podrán recibirse por el operador obligado en circuitos dedicados y claramente diferenciados de las llamadas telefónicas nacionales. La distinción deseada puede lograrse utilizando circuitos físicos separados o, virtualmente, distinguiendo las llamadas mediante señalización.

CAPÍTULO III

Medidas para evitar fraudes en el ámbito de los servicios de mensajería

Artículo 6. *Bloqueo de mensajes (SMS/MMS/RCS) que usan numeración que no haya sido atribuida, asignada o adjudicada, incluyendo numeración vacía.*

1. Los operadores deberán bloquear los mensajes (SMS/MMS/RCS) con CLI vacío o que presenten como CLI un número de teléfono español que no esté atribuido a ningún servicio o cuyo formato no sea coherente con el plan nacional de numeración telefónica, aprobado mediante Real Decreto 2296/2004, de 10 de diciembre, y sus disposiciones de desarrollo, las instrucciones sobre la utilización de recursos públicos de numeración para la prestación de servicios de mensajes cortos de texto y mensajes multimedia, establecidas en la Orden ITC/308/2008, de 31 de enero, el plan internacional de numeración descrito en la recomendación E.164 del Sector de Normalización de las Telecomunicaciones de la Unión Internacional de Telecomunicaciones (UIT-T), y cualquier otro plan de numeración que se determine por orden del Ministerio para la Transformación Digital y de la Función Pública.

2. Los operadores deberán bloquear los mensajes (SMS/MMS/RCS) que presenten como CLI numeraciones que no hayan sido asignadas por la Comisión Nacional de los Mercados y la Competencia a ningún operador o proveedor de servicios de comunicaciones electrónicas, para lo que deberán consultar la correspondiente base de datos gestionada por dicha comisión.

3. Asimismo, cada operador deberá bloquear los mensajes (SMS/MMS/RCS) que presenten como CLI numeraciones que le hayan sido asignadas, subasignadas o portadas y que ese operador todavía no haya adjudicado a ningún cliente.

La Comisión Nacional de los Mercados y la Competencia establecerá el mecanismo para aquellos casos en los que un operador tenga revendedores en su red a quienes les haya subasignado numeración, sin que se produzca un intercambio de información comercial entre competidores.

4. Este artículo se aplica independientemente de si el mensaje se envía dentro de España o entra en España desde el extranjero a través de una interfaz internacional de interconexión.

5. Por resolución de la persona titular de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales podrá exceptuarse de la obligación de bloqueo determinados supuestos debidamente justificados.

Las excepciones se notificarán a la Comisión Nacional de los Mercados y la Competencia, y se publicarán en el portal de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales.

Artículo 7. *Bloqueo de SMS/MMS/RCS con origen internacional.*

1. Los proveedores de redes y servicios involucrados en los servicios de mensajería SMS/MMS/RCS deberán bloquear cualquier mensaje SMS/MMS/RCS, recibido desde el extranjero a través de una interfaz internacional de interconexión cuando presenten como CLI un número de teléfono español, salvo que se trate de un caso de itinerancia internacional. La comprobación de si se trata de un caso de itinerancia internacional deberá llevarse a cabo por el operador a través de los instrumentos, mecanismos y procedimientos que tenga implementados a tal fin.

2. Los proveedores de redes y servicios involucrados en los servicios de mensajería SMS/MMS/RCS deberán bloquear cualquier mensaje SMS/MMS/RCS, recibido desde el extranjero a través de una interfaz internacional de interconexión cuando presenten un alias español, salvo que se trate de un caso de itinerancia internacional. La comprobación de si se trata de un caso de itinerancia internacional deberá llevarse a cabo por el operador a través de los instrumentos, mecanismos y procedimientos que tenga implementados a tal fin.

En el supuesto de recibirse un alias de una empresa extranjera no inscrito en el registro al que se refiere el artículo 8 por una interfaz internacional de interconexión deberá asimismo bloquearse, excepto si el abonado receptor del mensaje se encuentra en itinerancia, en cuyo caso, la Comisión Nacional de los Mercados y la Competencia establecerá la actuación más adecuada en función de las capacidades técnicas.

Artículo 8. *Registro de alias y bloqueo de SMS/MMS/RCS con alias no registrados o emitidos por entidades no habilitadas.*

1. Las empresas y administraciones que utilicen alias o los proveedores de servicios de mensajería actuando en su nombre, deberán inscribir dichos alias, con carácter previo a su utilización, en el correspondiente registro gestionado por la Comisión Nacional de los Mercados y la Competencia.

2. El registro contendrá junto con el alias, la identificación de aquellos proveedores de servicios de mensajería habilitados para el envío y transmisión de SMS/MMS/RCS utilizando como identificador el alias inscrito.

3. Los proveedores de redes y servicios involucrados en la transmisión de servicios de mensajería SMS/MMS/RCS deberán bloquear aquellos mensajes SMS/MMS/RCS identificados mediante alias que no hayan sido inscritos en el registro, o que habiendo sido inscritos no hayan sido recibidos de proveedores habilitados en dicho Registro para su envío o transmisión.

4. La Comisión Nacional de los Mercados y la Competencia dictará instrucciones sobre los sujetos obligados, el procedimiento, los requisitos y plazos del proceso de inscripción.

CAPÍTULO IV

Medidas para garantizar la correcta identificación de la numeración utilizada para la prestación de servicios de atención a clientes y la realización de llamadas comerciales no solicitadas

Artículo 9. *Prohibición de utilización de la numeración móvil para llamadas de atención al cliente o para la realización de llamadas comerciales no solicitadas.*

1. Se prohíbe la utilización de rangos de numeración atribuidos al servicio de comunicaciones móviles para la prestación de servicios de atención al cliente y para la realización de llamadas comerciales no solicitadas.

2. El incumplimiento de la prohibición establecida en el apartado 1 será sancionado conforme a lo establecido en el artículo 107.19 de la Ley 11/2022, de 28 de junio, General de Telecomunicaciones.

Artículo 10. *Atribución de los rangos 800 y 900 para la prestación del servicio de atención a clientes y para la realización de llamadas comerciales no solicitadas.*

1. Se atribuye los segmentos N=8 y 9, para el valor cero de las cifras X e Y, del plan nacional de numeración telefónica, además de a los servicios de cobro revertido automático,

a los servicios de atención a clientes y a la realización de llamadas comerciales no solicitadas.

2. Las llamadas desde las numeraciones pertenecientes al rango NXY 800 y 900 continuarán siendo gratuitas para el llamante.

3. Se autoriza, con carácter general, la utilización de numeración 800 y 900 en el campo del CLI, de acuerdo al artículo 61.2 y 71 del Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, aprobado por Real Decreto 424/2005, de 15 de abril, con objeto de que el usuario llamado pueda devolver las llamadas a estos números de forma gratuita.

Disposición adicional primera. *Remisión de estadísticas.*

Los sujetos obligados deberán remitir, por medios electrónicos, a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales y a la Comisión Nacional de los Mercados y la Competencia, con carácter anual, o cuando de manera excepcional, sean requeridos expresamente para ello, estadísticas de llamadas y mensajes bloqueados, desglosando, cuando sea técnicamente viable, el motivo del bloqueo.

Disposición adicional segunda. *Tratamiento de datos de carácter personal.*

Todos los tratamientos de datos de carácter personal derivados de la aplicación de la presente Orden Ministerial, se realizarán con estricta sujeción a lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales, y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, y en la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales, garantizando el derecho fundamental de los afectados a la protección de sus datos de carácter personal.

Disposición final primera. *Título competencial.*

Esta orden se dicta al amparo de la competencia exclusiva del Estado en materia de telecomunicaciones reconocida en el artículo 149.1.21.ª de la Constitución.

Disposición final segunda. *Modificación de la Resolución de 27 de mayo de 2013, de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, por la que se modifica la atribución de los rangos de numeración para comunicaciones móviles.*

1. Se modifica el apartado Primero.1.b) de la Resolución de 27 de mayo de 2013, de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, por la que se modifica la atribución de los rangos de numeración para comunicaciones móviles, que queda redactado de la siguiente manera:

> «b) La provisión de servicios asociados a redes públicas de comunicaciones móviles como son, entre otros, la prestación de servicios de red privada virtual soportados sobre redes de comunicaciones móviles, o su empleo en facilidades del tipo multilínea o multidispositivo.»

2. El apartado modificado en esta disposición final podrá ser modificado mediante resolución dictada por el mismo órgano que dictó la resolución en que figura.

Disposición final tercera. *Entrada en vigor.*

1. Esta orden entrará en vigor a los veinte días de su publicación en el «Boletín Oficial del Estado».

2. La obligación establecida en los artículos 5.1 y 7.1 de la presente orden deberá cumplirse en el plazo máximo de tres meses desde su entrada en vigor.

3. Los artículos 7.2 y 8 de la presente orden producirá efectos a los quince meses de su entrada en vigor.

4. El artículo 9 de la presente orden producirá efectos a los tres meses de su entrada en vigor.

§ 36

Real Decreto 1163/2005, de 30 de septiembre, por el que se regula el distintivo público de confianza en los servicios de la sociedad de la información y de comercio electrónico, así como los requisitos y el procedimiento de concesión

Ministerio de la Presidencia
«BOE» núm. 241, de 8 de octubre de 2005
Última modificación: 25 de febrero de 2008
Referencia: BOE-A-2005-16699

El Real Decreto 292/2004, de 20 de febrero, por el que se crea el distintivo público de confianza en los servicios de la sociedad de la información y de comercio electrónico y se regulan los requisitos y procedimiento de concesión, llevó a efecto la previsión contenida en la disposición final octava de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, para la aprobación de un distintivo de identificación de los códigos de conducta que ofrezcan determinadas garantías a los consumidores y usuarios.

La norma adoptada atribuye a la Administración General del Estado, a través del Instituto Nacional del Consumo, las competencias para los actos de concesión y retirada de este distintivo público en sus artículos 10 y 11 y en su disposición transitoria única. En los artículos 8.3 y 9 se atribuyen, en exclusiva, al Instituto Nacional del Consumo competencias relativas al seguimiento de la supervisión del cumplimiento de los códigos y de las obligaciones de las entidades promotoras de estos. La disposición final segunda, por último, atribuye al Presidente del Instituto Nacional del Consumo las competencias para adoptar las resoluciones precisas para la aplicación de lo dispuesto en dicho real decreto.

Por otra parte, en su artículo 5.2 se establece la previsión de que se favorezca e impulse la oferta al consumidor o usuario de la posibilidad de elegir, entre las lenguas oficiales de la Unión Europea, aquella en la que se han de realizar las comunicaciones comerciales, en especial, la información precontractual y el contrato.

El Consejo de Ministros ha atendido un requerimiento de incompetencia realizado por el Gobierno de la Generalidad de Cataluña que se concreta en solicitar del Gobierno de la Nación que adopte el acuerdo de derogar los artículos 5.2, 10 y 11, la disposición final segunda y las referencias al Instituto Nacional del Consumo contenidas en los artículos 8.3 y 9 del Real Decreto 292/2004, de 20 de febrero, o, subsidiariamente, el de darles nueva redacción en la que se reconozca la competencia de las comunidades autónomas respecto del procedimiento y funciones ejecutivas en ellos regulados y, en cuanto al artículo 5.2, se añada la referencia a las lenguas cooficiales en el territorio español. En efecto, en su reunión de 4 de junio de 2004, dicho órgano colegiado acordó aceptar tal requerimiento en los términos que a continuación se exponen.

En el precitado acuerdo considera el Gobierno que debe reconocerse la competencia de las comunidades autónomas respecto de los actos de concesión y de retirada del distintivo

de referencia (artículos 10 y 11 del Real Decreto 292/2004, de 20 de febrero) pues constituyen dichas concesiones actos de mera ejecución, una vez verificado el cumplimiento de los requisitos y condiciones correspondientes a los códigos de conducta que permitan su utilización y que se establecen en la norma requerida.

En consecuencia, y sin excluir la competencia de que el Estado dispone para crear o aprobar un distintivo que permita identificar aquellos prestadores de servicios de la sociedad de la información que voluntariamente se adhieran y respeten unos códigos de conducta de ámbito nacional o superior, cuyos requisitos mínimos u optativos deben ser fijados por el Estado, se debe cumplir el mandato de la disposición final octava de la Ley 34/2002, de 11 de julio, y, de acuerdo con la doctrina constitucional, considera el Gobierno que procede aceptar el requerimiento de incompetencia respecto a los artículos 10 y 11 y la disposición transitoria única y, por ende, respecto a las menciones al Instituto Nacional del Consumo contenidas en los artículos 8.3 y 9, así como en lo relativo a la disposición final segunda del real decreto requerido, por lo que procede modificar dichos preceptos para acomodarlos al reparto competencial. Se mantiene, no obstante, la comunicación al Instituto Nacional del Consumo de la información relevante a los efectos de la publicidad del distintivo o su comunicación a la Comisión de Cooperación de Consumo, en el marco de la necesaria cooperación institucional.

Por último, en cuanto a la modificación que se solicita en el requerimiento de incompetencia del tenor del ar-tículo 5.2 del real decreto requerido, considera el Gobierno que en este punto no existe una «vindicatio potestatis» propia de los conflictos positivos de competencia encaminados a eliminar transgresiones concretas y efectivas de los respectivos ámbitos competenciales, tal y como establece la jurisprudencia constitucional.

El cumplimiento de este acuerdo del Consejo de Ministros exige, en consecuencia, modificar el Real Decreto 292/2004, de 20 de febrero, para acomodar los artículos 10 y 11, y la disposición transitoria única y las menciones al Instituto Nacional del Consumo contenidas en los artículos 8.3 y 9, así como la disposición final segunda, al reparto competencial.

Para facilitar la aplicación de la norma, no obstante, se ha considerado necesario establecer en un único texto normativo la regulación del distintivo público de confianza en línea, y derogar el Real Decreto 292/2004, de 20 de febrero, cuya regulación no afectada por el requerimiento de incompetencia se incorpora a este real decreto.

En la tramitación de este real decreto se ha tenido en cuenta el parecer de las comunidades autónomas y ha sido oído el Consejo de Consumidores y Usuarios.

En su virtud, a propuesta de los Ministros de Sanidad y Consumo y de Industria, Turismo y Comercio, con la aprobación previa del Ministro de Administraciones Públicas, de acuerdo con el Consejo de Estado y previa deliberación en Consejo de Ministros en su reunión del día 30 de septiembre de 2005,

D I S P O N G O :

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

Este real decreto tiene por objeto regular el distintivo que podrán mostrar los prestadores de servicios que se adhieran a códigos de conducta que cumplan las condiciones previstas en el capítulo II de este real decreto, en cumplimiento de lo previsto en la disposición final octava de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

Asimismo, este real decreto establece las condiciones que deben reunir tales códigos de conducta, la concesión y retirada del distintivo y el procedimiento aplicable.

Artículo 2. *Denominación y forma del distintivo.*

Este distintivo se denominará «distintivo público de confianza en línea». Su formato es el que figura en el anexo.

Artículo 3. *Ámbito de aplicación.*

Este real decreto se aplica a las corporaciones, asociaciones u organizaciones comerciales, profesionales y de consumidores que adopten códigos de conducta destinados a regular las relaciones entre prestadores de servicios de la sociedad de la información y los consumidores y usuarios, cuando la adhesión a tales códigos conceda el derecho al uso y administración del «distintivo público de confianza en línea».

Este real decreto se aplicará, asimismo, a los prestadores de servicios de la sociedad de la información que hagan uso de dicho distintivo.

CAPÍTULO II

Requisitos de los códigos de conducta

Artículo 4. *Ámbito y contenido de los códigos.*

1. Los códigos de conducta de ámbito nacional o superior regulados por este real decreto deberán estar redactados en términos claros y accesibles.

2. Además de los otros requisitos exigidos en este real decreto, los códigos de conducta deben respetar la legalidad vigente e incluir, como mínimo, con suficiente grado de precisión:

a) Las garantías concretas que ofrecen a los consumidores y usuarios que mejoren o incrementen las reconocidas por el ordenamiento jurídico.

b) Un sistema de resolución extrajudicial de conflictos de entre los previstos en el artículo 7.

c) Los compromisos específicos que asumen los prestadores de servicios adheridos en relación con los problemas concretos planteados a los consumidores y usuarios del sector, identificados según la información de los promotores del código y la que, al efecto, les faciliten las asociaciones de consumidores y las Administraciones públicas sobre las reclamaciones presentadas por los consumidores y usuarios.

d) El ámbito de las actividades del prestador de servicios sometidas al código, que, al menos, englobará alguna de las siguientes áreas: las comunicaciones comerciales o la información precontractual, la contratación y los procedimientos de solución de quejas o reclamaciones, cuando estos sean distintos de los sistemas de resolución extrajudicial de conflictos a los que se refiere el artículo 7.

3. Estos códigos de conducta deberán prever la posibilidad de adhesión al código de prestadores de servicios que no sean miembros de la entidad promotora, siempre que la actividad desarrollada por estos esté incluida en el ámbito del código.

Artículo 5. *Compromisos adicionales.*

1. Sin perjuicio de cualquier otro compromiso que puedan establecer las entidades promotoras de los códigos de conducta regulados por este real decreto, estos podrán contener previsiones específicas sobre:

a) El grado de accesibilidad a los contenidos de los consumidores y usuarios que tengan alguna discapacidad o de edad avanzada, conforme a los criterios de accesibilidad generalmente reconocidos, así como los calendarios adoptados para el establecimiento de medidas adicionales.

b) Las medidas concretas adoptadas en materia de protección de los menores y de respeto a la dignidad humana y a los valores y derechos constitucionalmente reconocidos.

c) La adhesión a códigos de conducta sobre clasificación y etiquetado de contenidos. En tales casos, deberá facilitarse información completa sobre tales códigos.

d) Las instrucciones sobre los sistemas de filtrado de contenidos utilizables en las relaciones con los prestadores de servicios.

e) Los procedimientos previstos para comprobar que los prestadores de servicios reúnen las condiciones exigidas para la adhesión al código de conducta y la utilización del distintivo.

2. Las entidades promotoras de los códigos de conducta impulsarán que los prestadores de servicios adheridos ofrezcan al consumidor o usuario la posibilidad de elegir, entre las

lenguas oficiales de la Unión Europea, la lengua en que se han de realizar las comunicaciones comerciales y, en especial, la información precontractual y el contrato.

Artículo 6. *Participación del Consejo de Consumidores y Usuarios.*

En la elaboración y modificación de los códigos de conducta regulados en este real decreto deberá darse participación al Consejo de Consumidores y Usuarios. Esta participación se articulará, como mínimo, de la siguiente forma:

a) Que, con carácter previo a la redacción del código de conducta, las entidades promotoras de este pongan en conocimiento del Consejo su voluntad de adoptarlo y soliciten la colaboración de este órgano a través del procedimiento que, en cada caso, se acuerde.

b) Que las entidades promotoras soliciten a las asociaciones de consumidores y usuarios, a través del Consejo, la identificación de los problemas específicos del sector, partiendo de las reclamaciones y consultas por ellas tramitadas, y a los efectos previstos en el artículo 4.2.c).

c) Que el Consejo no emita motivadamente un dictamen desfavorable sobre el contenido definitivo del código de conducta en el plazo de un mes desde que la entidad promotora se lo hubiera solicitado. La mera formulación de observaciones al código no supone la emisión de un dictamen desfavorable. El dictamen desfavorable únicamente podrá fundarse en el incumplimiento de los requisitos recogidos en este real decreto o en las normas de protección a los consumidores y usuarios.

Artículo 7. *Sistemas de resolución extrajudicial de conflictos.*

1. Los códigos de conducta que pretendan obtener el «distintivo público de confianza en línea» deberán establecer, como medio de solución de controversias entre los prestadores de servicios y los consumidores y usuarios, el sistema arbitral de consumo u otro sistema de resolución extrajudicial de conflictos que figure en la lista que publica la Comisión Europea sobre sistemas alternativos de resolución de conflictos con consumidores y que respete los principios establecidos por la normativa comunitaria a este respecto.

2. En los procedimientos de resolución extrajudicial de conflictos a que hace referencia el apartado anterior, podrá hacerse uso de medios electrónicos en la medida en que lo posibilite su normativa específica y con las condiciones previstas en ella.

3. La adhesión de los prestadores de servicios a uno de los sistemas mencionados en el apartado anterior es requisito necesario para la incorporación de los prestadores de servicios a los códigos de conducta.

Artículo 8. *Supervisión del cumplimiento de los códigos de conducta por los prestadores adheridos.*

1. Los códigos de conducta deberán incluir procedimientos de evaluación independientes para comprobar el cumplimiento de las obligaciones asumidas por los prestadores de servicios adheridos, y establecer un régimen sancionador adecuado, eficaz y disuasorio.

2. El procedimiento de evaluación que se prevea, que podrá realizarse íntegramente por medios electrónicos, deberá garantizar:

a) La independencia e imparcialidad del órgano responsable de la evaluación y sanción.

b) La sencillez, accesibilidad y gratuidad para la presentación de quejas y reclamaciones ante dicho órgano por los eventuales incumplimientos del código de conducta y la celeridad en todas las fases del procedimiento.

c) La audiencia del reclamado y el principio de contradicción.

d) Una graduación de sanciones que permita ajustarlas a la gravedad del incumplimiento. Esas sanciones deberán ser disuasorias, y podrá establecerse, en su caso, su publicidad o la suspensión o expulsión de la adhesión al código o a la entidad promotora, en el caso de que se trate de prestadores de servicios integrados en ella.

e) La notificación al denunciante de la solución adoptada.

3. Las sanciones que se impongan a los prestadores de servicios por incumplimiento de los códigos de conducta deberán notificarse trimestralmente al órgano administrativo competente para la concesión y retirada del distintivo. Cuando dichas sanciones supongan la

expulsión de la adhesión al código o la suspensión de sus derechos, la notificación deberá realizarse en el plazo de los cinco días siguientes a la adopción de la sanción.

CAPÍTULO III

Obligaciones de las entidades promotoras

Artículo 9. *Obligaciones de las entidades promotoras de los códigos de conducta.*

Las entidades promotoras de códigos de conducta regulados en este real decreto tendrán las siguientes obligaciones:

a) Administrar el «distintivo público de confianza en línea», facilitar y gestionar su utilización por los prestadores de servicios adheridos al código de conducta adoptado por ellas y que, conforme a lo previsto en el artículo 7.3, le acrediten su adhesión al sistema extrajudicial de resolución de conflictos previsto en el código de conducta. Las entidades promotoras, asimismo, deberán informar al órgano administrativo competente para la concesión y retirada del distintivo sobre las adhesiones al código de conducta de nuevos proveedores de servicios o sobre las bajas, mediante la comunicación quincenal de las variaciones producidas.

b) Mantener accesible al público información actualizada sobre las entidades promotoras, el contenido del código de conducta, los procedimientos de adhesión y de denuncia frente a posibles incumplimientos del código, los sistemas de resolución extrajudicial de conflictos que promueve el código y los prestadores de servicios adheridos a este en cada momento.

Esta información deberá presentarse de forma concisa y clara y estar permanentemente accesible por medios electrónicos.

c) Remitir al órgano administrativo competente para la concesión y retirada del distintivo una memoria anual sobre las actividades realizadas para difundir el código de conducta y promover la adhesión a este, las actuaciones de verificación del cumplimiento del código y sus resultados, las quejas y reclamaciones tramitadas y el curso que se les hubiera dado, las sanciones impuestas y cualquier otro aspecto que las entidades promotoras deseen destacar.

d) Evaluar periódicamente la eficacia del código de conducta, midiendo el grado de satisfacción de los consumidores y usuarios y, en su caso, actualizar su contenido para adaptarlo a los cambios experimentados en la tecnología, en la prestación y uso de los servicios de la sociedad de la información y en la normativa que les sea aplicable.

Esta evaluación deberá contar con la participación del Consejo de Consumidores y Usuarios en los términos previstos en el artículo 6 y tendrá lugar, al menos, cada cuatro años, salvo que sea precisa la adaptación de los compromisos del código a la modificación de la normativa aplicable en un plazo menor.

Los resultados de la evaluación se comunicarán a la Comisión Europea y al órgano administrativo competente para la concesión y retirada del distintivo.

e) Favorecer la accesibilidad de las personas que tengan alguna discapacidad o sean de edad avanzada a toda la información disponible sobre el código de conducta.

CAPÍTULO IV

Concesión y retirada del distintivo

Artículo 10. *Órgano competente para la concesión y retirada del distintivo.*

La concesión y retirada del distintivo de confianza regulado en este real decreto, así como el ejercicio de las funciones dirigidas a velar por el mantenimiento de los requisitos que justifican su otorgamiento, corresponde al órgano competente en materia de consumo de la comunidad autónoma en que esté domiciliada la entidad promotora del código. Estas resoluciones tendrán validez en todo el territorio del Estado.

A los efectos de la publicidad del distintivo prevista en el artículo 13, estos órganos deberán comunicar al Instituto Nacional del Consumo los actos de concesión o retirada del distintivo, dándole traslado de toda la información precisa para cumplir con las obligaciones

impuestas por el citado precepto, en los cinco días siguientes a la adopción de las respectivas resoluciones. En idéntico plazo, a los efectos de la publicidad y del establecimiento de la necesaria cooperación administrativa a través de la Comisión de Cooperación de Consumo, tales órganos competentes darán traslado al Instituto Nacional del Consumo de la información que le hayan facilitado las entidades promotoras conforme a los artículos 8.3 y 9.a), c) y d).

Artículo 11. *Otorgamiento del distintivo.*

1. Las entidades promotoras de los códigos de conducta regulados en este real decreto presentarán su solicitud ante el órgano administrativo competente para la concesión y retirada del distintivo, a la que acompañarán de una copia del código, de la documentación acreditativa de la participación del Consejo de Consumidores y Usuarios y, en su caso, de haberse comunicado el proyecto de código a la Comisión Europea.

Asimismo, deberán aportar la documentación relativa a la adhesión de los prestadores de servicios que lo hayan suscrito al sistema extrajudicial de resolución de litigios que se prevea en el código.

2. En la tramitación de este procedimiento, el órgano competente para la concesión y retirada del «distintivo público de confianza en línea» podrá requerir cuantos informes estime pertinentes para valorar el alcance y contenido del código de conducta presentado y, en todo caso, con carácter preceptivo, el informe del Ministerio de Industria, Turismo y Comercio y de la Comisión de Cooperación de Consumo. En el caso de tratarse de códigos de conducta que afecten a actividades de venta a distancia deberá solicitarse el informe preceptivo de los órganos competentes en materia de inscripción, registro y control de estas empresas.

Asimismo, el órgano administrativo competente para la concesión y retirada del distintivo podrá solicitar el informe de los órganos competentes en materia de defensa de la competencia cuando, por el alcance y contenido del código, surgieran dudas sobre si puede afectar negativamente a la competencia.

3. Las resoluciones que se dicten en este procedimiento deberán ser motivadas y se publicarán en el diario oficial de la comunidad autónoma competente, conforme a lo previsto en el artículo 10, y en el «Boletín Oficial del Estado».

Dichas resoluciones serán recurribles conforme a lo previsto en el capítulo II del título VII de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Artículo 12. *Retirada del distintivo público de confianza.*

El derecho a la utilización y administración del «distintivo público de confianza en línea» podrá ser retirado si las entidades promotoras de los códigos de conducta reconocidos incumplen las obligaciones establecidas en este real decreto. La retirada del derecho a la utilización y administración del «distintivo público de confianza en línea» a una entidad promotora implicará la imposibilidad de su utilización por parte de los prestadores de servicios adheridos al código de conducta.

Asimismo, ante la inactividad de la entidad promotora y sin perjuicio de las medidas que pudieran adoptarse frente a ella por tal causa, podrá retirarse directamente el uso del distintivo a los prestadores de servicios que incumplan manifiesta y reiteradamente el código de conducta cuya adhesión les confiera tal derecho.

La retirada del distintivo de confianza se tramitará mediante un procedimiento contradictorio y contará con el informe preceptivo de la Comisión de Cooperación de Consumo; asimismo, podrá adoptarse como medida provisional la suspensión del derecho a utilizar el distintivo. La resolución por la que se retire el distintivo será recurrible conforme a lo previsto en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Artículo 13. *Publicidad del distintivo.*

1. El Instituto Nacional del Consumo publicará en su página de Internet los códigos de conducta a los que se conceda el distintivo regulado en este real decreto; la relación de las entidades promotoras de dichos códigos y la de los prestadores de servicios adheridos; las

sanciones impuestas a los prestadores de servicios por incumplimiento, si son públicas, especialmente cuando lleven aparejada la suspensión o expulsión del prestador de servicios del código o de la entidad promotora o la retirada del «distintivo público de confianza en línea», y la dirección establecida para la presentación de quejas por incumplimiento de los códigos y la de los órganos de resolución extrajudicial de conflictos previstos en los códigos de conducta.

2. Las entidades promotoras de los códigos de conducta a las que se haya concedido el derecho a la utilización y administración del distintivo regulado en este real decreto y los prestadores de servicios adheridos a tales códigos podrán usar, tanto gráficamente como por su denominación, el «distintivo público de confianza en línea» en todas sus manifestaciones internas y externas, incluidas las campañas de publicidad. Todo ello sin perjuicio del cumplimiento de las obligaciones de información al consumidor, en particular, en relación con la adhesión a sistemas extrajudiciales de resolución de conflictos.

3. Las entidades promotoras y los prestadores de servicios adheridos a los códigos de conducta deberán posibilitar el acceso al contenido del código y a la dirección habilitada para presentar las quejas y reclamaciones a través de los soportes informáticos en los que se inserte el «distintivo público de confianza en línea».

CAPÍTULO V

Actuaciones de control

Artículo 14. *Actuaciones de control.*

Cuando la utilización del «distintivo público de confianza en línea», contraviniendo lo dispuesto en este real decreto, constituya publicidad ilícita, el Instituto Nacional del Consumo y los órganos competentes en materia de consumo de las comunidades autónomas podrán iniciar el procedimiento sancionador o promover el ejercicio de las acciones judiciales que procedan, de conformidad con lo previsto en la Ley 26/1984, de 19 de julio, General para la Defensa de los Consumidores y Usuarios, en el Real Decreto 1945/1983, de 22 de junio, por el que se regulan las infracciones y sanciones en materia defensa del consumidor y de la producción agroalimentaria, en la Ley 34/1988, de 11 de noviembre, General de Publicidad, o en las respectivas leyes autonómicas.

Disposición transitoria primera. *Adaptación de los códigos vigentes.*

Hasta el 31 de julio de 2006, las entidades promotoras de códigos vigentes en la fecha de entrada en vigor de este real decreto podrán solicitar la concesión del «distintivo público de confianza en línea», acreditando, en su caso, que se ha comunicado el proyecto adaptado a la Comisión Europea.

En tales supuestos, no será exigible la notificación previa al Consejo de Consumidores y Usuarios prevista en el artículo 6.a), y bastará con que se requiera la colaboración de dicho órgano, a través del procedimiento que en cada caso se acuerde, para la realización de las adaptaciones precisas para cumplir los requisitos exigidos en este real decreto.

Disposición transitoria segunda. *Período transitorio.*

1. Las disposiciones de este real decreto serán de aplicación a todos los procedimientos de concesión o retirada que estén en tramitación a su entrada en vigor. A tales efectos, el Instituto Nacional del Consumo trasladará al órgano competente para la concesión o retirada del «distintivo público de confianza en línea» la documentación que obre en su poder, y se abstendrá de realizar cualquier otra actuación de impulso del procedimiento.

2. Los «distintivos públicos de confianza en línea» que se hubieran concedido conforme a la normativa aplicable con anterioridad a la entrada en vigor de este real decreto mantendrán toda su vigencia. El Instituto Nacional del Consumo trasladará al órgano competente en cada caso toda la documentación que obre en su poder respecto de tales procedimientos al objeto de que dicho órgano ejerza las funciones de vigilancia que le atribuye el artículo 10.

3. Las solicitudes que se formulen tras la entrada en vigor de este real decreto se realizarán ante el órgano competente, conforme al artículo 10.

Disposición derogatoria única. *Derogación del Real Decreto 292/2004, de 20 de febrero.*

Se deroga el Real Decreto 292/2004, de 20 de febrero, por el que se crea el distintivo público de confianza en los servicios de la sociedad de la información y de comercio electrónico y se regulan los requisitos y procedimiento de concesión.

Disposición final primera. *Título y habilitación competencial.*

Este real decreto se dicta al amparo del artículo 149.1.1.ª, 6.ª, 8.ª y 21.ª de la Constitución y en ejecución de lo dispuesto en la disposición final octava de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

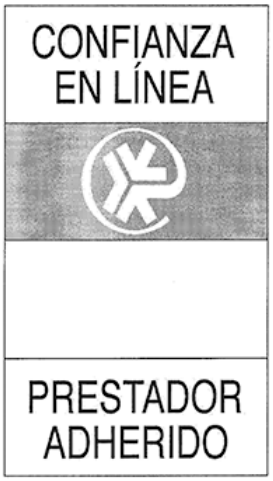
Disposición final segunda. *Facultad de aplicación.*

Los órganos competentes de las comunidades autónomas podrán adoptar las resoluciones precisas para la aplicación de lo dispuesto en este real decreto, en particular aquellas que posibiliten la gestión íntegra de los procedimientos previstos en él mediante la utilización de técnicas electrónicas, informáticas y telemáticas, de conformidad con lo previsto en la normativa vigente.

Disposición final tercera. *Entrada en vigor.*

El presente real decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

ANEXO



Denominación: Distintivo público de confianza en línea.

Construcción gráfica:

Una figura vertical constituida por cuatro rectángulos iguales de 45 mm de base por 20,25 de altura. Las medidas totales exteriores incluidos los cuatro elementos son 45 mm de base por 81 mm de altura. El segundo recuadro contiene una imagen mixta representativa de la expresión abreviada de la arroba y el logotipo de Arbitraje de Consumo.

Los rectángulos superior e inferior contienen los siguientes textos: el superior CONFIANZA EN LÍNEA y el inferior PROVEEDOR ADHERIDO, ambos en mayúsculas. El tercer recuadro, opcional, es un espacio en blanco para situar distintos logotipos.

Tipografía: helvética. Estilo: normal. Cuerpo de letra: 22. Interlineado: sólido. Escala horizontal: 100

Colores: naranja y negro. El primero compuesto por magenta 47% y amarillo 100 % y el segundo negro base. El logotipo arriba descrito figura calado en blanco sobre fondo naranja.

Si se prescinde del recuadro blanco opcional, el conjunto del logotipo.

Todas las líneas que forman el conjunto son en color negro de 0,5 puntos.

Si se prescinde del recuadro blanco opcional las medidas del conjunto del logotipo deben ser de 45 mm de base por 61 mm de altura.

Para su uso en Internet se establece un tamaño mínimo en píxeles de 75 de ancho por 134 de altura, en la versión completa y de 48 de ancho por 65 de altura prescindiendo del recuadro opcional. Se deben guardar las mismas proporciones en tamaños superiores.

§ 37

Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos

Ministerio de la Presidencia, Relaciones con las Cortes y Memoria Democrática
«BOE» núm. 77, de 31 de marzo de 2021
Última modificación: 2 de abril de 2025
Referencia: BOE-A-2021-5032

La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, consagran el derecho de las personas a relacionarse por medios electrónicos con las administraciones públicas, simplificando el acceso a los mismos, y refuerzan el empleo de las tecnologías de la información y las comunicaciones (TIC) en las administraciones públicas, tanto para mejorar la eficiencia de su gestión como para potenciar y favorecer las relaciones de colaboración y cooperación entre ellas.

Ambas leyes recogen los elementos que conforman el marco jurídico para el funcionamiento electrónico de las Administraciones Públicas introduciendo un nuevo paradigma que supera la concepción que inspiró la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos y su desarrollo reglamentario parcial en la Administración General del Estado y sus organismos públicos vinculados o dependientes a través del Real Decreto 1671/2009, de 6 de noviembre, según la cual la tramitación electrónica no era sino una forma de gestión de los procedimientos.

En este sentido, la Ley 11/2007, de 22 de junio, respondiendo a las nuevas realidades, exigencias y experiencias que se habían puesto de manifiesto, al propio desarrollo de la sociedad de la información y al cambio de circunstancias tecnológicas y sociales, entre otros factores, reconocía el derecho de la ciudadanía a relacionarse electrónicamente con las Administraciones Públicas, y no solo la posibilidad como se preveía en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. La Ley 11/2007, de 22 de junio admitía incluso que, por vía reglamentaria, se estableciese la obligatoriedad de comunicarse con las Administraciones Públicas por medios electrónicos cuando las personas interesadas fuesen personas jurídicas o colectivos de personas físicas que por razón de su capacidad económica o técnica, dedicación profesional u otros motivos acreditados tuviesen garantizado el acceso y disponibilidad de los medios tecnológicos precisos.

En este contexto, la Ley 39/2015, de 1 de octubre, y la Ley 40/2015, de 1 de octubre, han dado respuesta a la demanda actual en el sentido de que la tramitación electrónica de los procedimientos debe constituir la actuación habitual de las Administraciones Públicas, y no solamente ser una forma especial de gestión de los mismos. En consecuencia, se prevé que las relaciones de las Administraciones entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes se realizará a través de medios electrónicos, y se

establece la obligatoriedad de relacionarse electrónicamente con la Administración para las personas jurídicas, entes sin personalidad y, en algunos supuestos, para las personas físicas, y ello sin perjuicio de la posibilidad de extender esta obligación a otros colectivos, por vía reglamentaria.

Con estos antecedentes, era necesario desarrollar y concretar las previsiones legales con el fin, entre otros aspectos, de facilitar a los agentes involucrados en el uso de medios tecnológicos su utilización efectiva, aclarando y precisando, al mismo tiempo, aquellas materias reguladas en estas leyes que permiten un margen de actuación reglamentaria.

La satisfacción del interesado, por tanto, en el uso de los servicios públicos digitales es fundamental para garantizar adecuadamente sus derechos y el cumplimiento de sus obligaciones en su relación con las Administraciones Públicas. Por ello, es prioritario disponer de servicios digitales fácilmente utilizables y accesibles, de modo que se pueda conseguir que la relación del interesado con la Administración a través del canal electrónico sea fácil, intuitiva, efectiva, eficiente y no discriminatoria.

Por otra parte, a lo largo de las dos últimas décadas, los sucesivos Gobiernos de España han ido adoptando programas para el avance digital alineados con las agendas digitales europeas, en todos los cuales ha estado presente el eje de mejora de la Administración electrónica. Fruto de estos programas, España cuenta con una posición muy favorable para abordar la siguiente fase del proceso de Transformación digital de nuestro país y, en lo que concierne a la Administración electrónica, está situada entre los países más avanzados de la Unión Europea, lo que se ha logrado gracias al esfuerzo continuado de las Administraciones Públicas en la adaptación de sus servicios electrónicos para ofrecer cada vez mejores servicios, más adaptados a las demandas de la ciudadanía y las empresas, y más eficientes. En este esfuerzo, la estrategia de España se ha basado en el impulso de los fundamentos que permiten una tramitación electrónica completa, y en el desarrollo de servicios que pueden ser utilizados libremente por todas las Administraciones Públicas, y que están alineados con los esquemas de interoperabilidad europeos.

Los cambios que se están produciendo con la maduración de tecnologías disruptivas y su aplicación a la gestión de la información y la ejecución de políticas públicas, los nuevos modelos de relación de la ciudadanía y empresas con las Administraciones y la reutilización eficiente de la información son grandes desafíos que para ser afrontados con éxito y para que coadyuven a la Transformación digital exigen como presupuesto contar con un marco regulatorio adecuado, tanto con rango de ley como con rango reglamentario, que garantizando la seguridad jurídica para todos los intervinientes sirva a los objetivos de mejorar la eficiencia administrativa para hacer efectiva una Administración totalmente electrónica e interconectada, incrementar la transparencia de la actuación administrativa y la participación de las personas en la Administración Electrónica y garantizar servicios digitales fácilmente utilizables.

En este sentido, la Agenda España Digital 2025 contiene un eje estratégico específico sobre la Transformación Digital del Sector Público, cuya plasmación se concreta en el cumplimiento de un conjunto de medidas entre las que se encuentra la mejora del marco regulatorio de la Administración digital y específicamente en la aprobación de este real decreto. Por su parte, el Plan de Recuperación, Transformación y Resiliencia (España Puede) incluye entre sus diez políticas palanca de reforma estructural para un crecimiento sostenible e inclusivo, lograr una Administración modernizada a través de su digitalización, tanto a nivel transversal como en ámbitos estratégicos, que actúe como tractor de los cambios tecnológicos. El último hito en estrategia transformadora lo constituye el Plan de Digitalización de las Administraciones Públicas 2021 -2025, que supone un salto decisivo en la mejora de la eficacia y eficiencia de la Administración Pública, en la transparencia y eliminación de trabas administrativas a través de la automatización de la gestión, en una mayor orientación a la personalización de servicios y a la experiencia de usuario, actuando todo ello de elemento catalizador de la innovación tecnológica de nuestro país desde el ámbito público.

En definitiva, el Reglamento que aprueba este real decreto persigue los cuatro grandes objetivos mencionados: mejorar la eficiencia administrativa, incrementar la transparencia y la participación, garantizar servicios digitales fácilmente utilizables y mejorar la seguridad jurídica.

En primer lugar, persigue mejorar la eficiencia administrativa para hacer efectiva una Administración totalmente electrónica e interconectada. Así, se desarrolla y concreta el empleo de los medios electrónicos establecidos en las leyes 39/2015, de 1 de octubre, y 40/2015, de 1 de octubre, para garantizar, por una parte, que los procedimientos administrativos se tramiten electrónicamente por la Administración y, por otra, que la ciudadanía se relacione con ella por estos medios en los supuestos en que sea establecido con carácter obligatorio o aquellos lo decidan voluntariamente.

Un segundo objetivo consiste en incrementar la transparencia de la actuación administrativa y la participación de las personas en la Administración Electrónica. Así, se desarrolla el funcionamiento del Punto de Acceso General electrónico (PAGe), y la Carpeta ciudadana en el Sector Público Estatal. Se regula el contenido y los servicios mínimos a prestar por las sedes electrónicas y sedes electrónicas asociadas y el funcionamiento de los registros electrónicos.

En tercer lugar, el Reglamento persigue garantizar servicios digitales fácilmente utilizables de modo que se pueda conseguir que la relación del interesado con la Administración sea fácil, intuitiva y efectiva cuando use el canal electrónico.

Por último, busca mejorar la seguridad jurídica. Así, se elimina la superposición de regímenes jurídicos distintos, se adapta e integra en el Reglamento que aprueba este real decreto la regulación que aún permanecía vigente del Real Decreto 1671/2009, de 6 de noviembre, procediendo, por ello, a su derogación definitiva y se adecua la regulación al nuevo marco de la Ley 39/2015, de 1 de octubre y la Ley 40/2015, de 1 de octubre.

El real decreto consta de un artículo único que aprueba el Reglamento de actuación y funcionamiento del Sector Público por medios electrónicos, dos disposiciones transitorias, una disposición derogatoria y cinco disposiciones finales.

Entre las cinco disposiciones finales hay dos que modifican normas vigentes y las tres restantes regulan el título competencial, la habilitación reglamentaria para el desarrollo y ejecución del real decreto y la entrada en vigor. Respecto de las disposiciones modificativas, estas afectan al Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica y al Real Decreto 931/2017, de 27 de octubre, por el que se regula la Memoria del Análisis de Impacto Normativo. Así, en primer lugar, con relación al Real Decreto 4/2010, de 8 de enero, su artículo 29 establece que el Esquema Nacional de Interoperabilidad se desarrollará y perfeccionará a lo largo del tiempo en paralelo al progreso de los servicios de Administración electrónica, la evolución tecnológica y a medida que vayan consolidándose las infraestructuras que lo apoyan. Por ello, la rápida evolución de las tecnologías, la experiencia derivada de la aplicación del Esquema Nacional de Interoperabilidad desde su aprobación hace 10 años, las previsiones de la Ley 39/2015, de 1 de octubre, y de la Ley 40/2015, de 1 de octubre, relativas a la interoperabilidad entre las Administraciones Públicas y sus órganos, organismos públicos y entidades de derecho público vinculados o dependientes, más la necesidad de adecuarse a lo previsto en el Reglamento n.º 1025/2012 del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, sobre la normalización europea, por el que se modifican las Directivas 89/686/CEE y 93/15/CEE del Consejo y las Directivas 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE y 2009/105/CE del Parlamento Europeo y del Consejo y por el que se deroga la Decisión 87/95/CEE del Consejo y la Decisión no 1673/2006/CE del Parlamento Europeo y del Consejo, determinan la necesidad de proceder a modificar ciertos aspectos de su redacción actual. En consecuencia, se modifican los artículos, 9, 11, 14, 16, 17, y 18, así como la disposición adicional primera y el anexo de glosario, a la vez que se suprimen el artículo 19 y las disposiciones adicionales tercera y cuarta.

En segundo lugar, se modifica el Real Decreto 931/2017, de 27 de octubre, para incorporar en la Memoria del Análisis de Impacto Normativo el análisis de la incidencia en los gastos en medios o servicios de la Administración digital dentro del impacto presupuestario de los proyectos y, por otra parte, para incluir dentro del apartado de «Otros impactos» el que tendrá para las personas destinatarias de la norma y para la organización y funcionamiento de la Administración el desarrollo o uso de los medios y servicios de la Administración digital que conlleve la aplicación de la normativa proyectada.

Por su parte, el Reglamento de actuación y funcionamiento del Sector Público por medios electrónicos que aprueba el real decreto consta de 65 artículos distribuidos en cuatro títulos, diez disposiciones adicionales y un anexo de definiciones.

El título preliminar del Reglamento comprende las disposiciones generales regulando el objeto y ámbito de aplicación de la norma (que se remite al ámbito del artículo 2 tanto de la Ley 39/2015, de 1 de octubre, como de la Ley 40/2015, de 1 de octubre) y los principios generales que debe respetar el sector público en sus actuaciones y relaciones electrónicas. Entre estos principios se incluyen el de neutralidad tecnológica y de adaptabilidad al progreso de las tecnologías y sistemas de comunicaciones electrónicas, para garantizar tanto la independencia en la elección de las alternativas tecnológicas necesarias para relacionarse con las Administraciones Públicas por parte de las personas interesadas y por el propio sector público, como la libertad para desarrollar e implantar los avances tecnológicos en un ámbito de libre mercado; el principio de accesibilidad, para promover que el diseño de los servicios electrónicos garantice la igualdad y no discriminación en el acceso de las personas usuarias, en particular, de las personas discapacitadas y de las personas mayores; el principio de facilidad de uso, que determina que el diseño de los servicios electrónicos esté centrado en las personas usuarias para minimizar el grado de conocimiento tecnológico necesario para el uso del servicio, el principio de interoperabilidad, entendido como la capacidad de los sistemas de información y,por ende, de los procedimientos a los que estos dan soporte, de compartir datos y posibilitar el intercambio de información entre ellos; el principio de proporcionalidad, para que las medidas de seguridad y garantías que se exijan sean adecuadas a la naturaleza y circunstancias de los distintos trámites y actuaciones electrónicos y, por último, el principio de personalización y proactividad, entendido como la capacidad de las Administraciones Públicas para que, partiendo del conocimiento adquirido del usuario final del servicio, proporcione servicios precumplimentados y se anticipe a las posibles necesidades de los mismos.

Asimismo el título preliminar regula el derecho y obligación de relacionarse electrónicamente con las Administraciones Públicas, en aplicación del artículo 14 de la Ley 39/2015, de 1 de octubre, y los canales a través de los cuales las Administraciones Públicas prestarán la asistencia necesaria para facilitar el acceso de las personas interesadas a los servicios electrónicos proporcionados en su ámbito.

El título I regula los portales de internet, el PAGe, las sedes electrónicas y sedes electrónicas asociadas (características, creación y supresión, contenido y servicios, y responsabilidad) y el área personalizada a través de la cual cada interesado podrá acceder a su información, al seguimiento de los trámites administrativos que le afecten y a las notificaciones y comunicaciones en el ámbito de la Administración Pública competente, que en el ámbito estatal se denomina «Carpeta Ciudadana».

El título II se subdivide en tres capítulos y regula el procedimiento administrativo por medios electrónicos. Así, el capítulo I, sobre «Disposiciones generales» aborda la tramitación administrativa automatizada y el régimen de subsanaciones. Por su parte el capítulo II regula la identificación y autenticación de las Administraciones Públicas y de las personas interesadas y se subdivide en cuatro Secciones: la 1ª aborda las disposiciones comunes a la identificación y autenticación y condiciones de interoperabilidad (incluyendo la plataforma de verificación de certificados electrónicos y otros sistemas de identificación), la 2.ª regula la «Identificación electrónica de las Administraciones Públicas y la autenticación del ejercicio de su competencia», que comprende la identificación de las sedes electrónicas y sedes asociadas, la identificación mediante sello electrónico basado en certificado electrónico cualificado, los sistemas de firma electrónica para la actuación administrativa automatizada, la identificación y firma del personal al servicio de las Administraciones Públicas (incluidos los certificados de empleado público con número de identificación profesional) y la autenticación e identificación de las Administraciones emisoras y receptoras en intercambio de datos a través de entornos cerrados de comunicación. La sección 3ª desarrolla la regulación de la identificación y firma de las personas interesadas y, por último, la sección 4ª regula la acreditación de la representación de las personas interesadas (regulando, entre otros extremos, el registro electrónico de apoderamientos).

El título II se cierra con el capítulo III, que en sus dos secciones regula los Registros electrónicos, las notificaciones electrónicas y los otros actos de comunicación electrónicos.

Así, la sección 1ª regula los registros electrónicos (entre otros aspectos, el Registro Electrónico General de cada Administración y la presentación y tratamiento de documentos en registro o las competencias de las Oficinas de asistencia en materia de registros de la Administración General del Estado) y la sección 2ª regula las comunicaciones administrativas a las personas interesadas por medios electrónicos (actos de comunicación electrónica a las personas interesadas distintos de las notificaciones o publicaciones) y las notificaciones electrónicas (incluyendo las reglas generales de la práctica de las notificaciones electrónicas, el aviso de puesta a disposición de la notificación, la notificación a través de la Dirección Electrónica Habilitada única (DEHu) y la notificación electrónica en sede electrónica o sede electrónica asociada).

El título III regula el expediente electrónico y se divide en dos capítulos. El capítulo I regula el documento administrativo electrónico y los requisitos y la emisión de copias auténticas de documentos públicos administrativos o documentos privados, que sean originales o copias auténticas de originales; la formación del expediente administrativo electrónico y el ejercicio de acceso al mismo y a la obtención de copias y la destrucción de documentos. Por su parte, el capítulo II regula la conservación de documentos electrónicos y la definición de archivo electrónico único.

Por último, el título IV se divide en dos capítulos y regula las relaciones y colaboración entre Administraciones Públicas para el funcionamiento electrónico del sector público. Así, el capítulo I aborda la colaboración entre las Administraciones Públicas para la actuación administrativa por medios electrónicos e incluye las obligadas relaciones interadministrativas e interorgánicas por medios electrónicos en el ejercicio de sus competencias, las comunicaciones en la Administración General del Estado, la posibilidad de adhesión a sedes electrónicas y sedes electrónicas asociadas y la regulación del Sistema de Interconexión de Registros (SIR), a través del cual deberán realizarse las interconexiones entre Registros de las Administraciones Públicas, que deberán ser interoperables entre sí y, en el caso de la Administración General del Estado, lo que supone una novedad, también con los sistemas de gestión de expedientes.

El capítulo I del título IV regula también las transmisiones de datos a las que se refiere el artículo 155 de la Ley 40/2015 de 1 de octubre, las plataformas de intermediación de datos (con mención especial a la de ámbito estatal), la remisión electrónica de expedientes administrativos en el ámbito de las Administraciones públicas mediante puesta a disposición, a través de un nodo de interoperabilidad, de la dirección electrónica o localizador que dé acceso al expediente electrónico completo y, por último, las previsiones el intercambio automático de datos o documentos a nivel europeo previstos en el Reglamento (UE) n.º 2018/1724 del Parlamento Europeo y del Consejo, de 2 de octubre de 2018, relativo a la creación de una pasarela digital única de acceso a información, procedimientos y servicios de asistencia y resolución de problemas y por el que se modifica el Reglamento (UE) n.º 1024/2012.

El título IV finaliza con el capítulo II, que regula la transferencia y uso compartido de tecnologías entre Administraciones Públicas, abordando, por una parte, la reutilización de sistemas y aplicaciones de las Administraciones Públicas y, por otra, la adhesión a las plataformas, registros o servicios electrónicos de la Administración General del Estado

La parte final del Reglamento consta de diez disposiciones adicionales y un anexo de definiciones. Las primeras regulan la obligatoriedad de uso de medios electrónicos en los procesos selectivos para el acceso al empleo público en el ámbito de la Administración General del Estado; la promoción de la formación del personal al servicio de la Administración General del Estado para garantizar el derecho de las personas interesadas a ser asistidas en el uso de medios electrónicos en sus relaciones con la Administración Pública; la creación del nodo de interoperabilidad para la identificación electrónica del Reino de España para el reconocimiento mutuo de identidades electrónicas entre Estados miembros de la Unión Europea; la adhesión de las entidades de derecho privado vinculadas o dependientes de la Administración General del Estado, en el ejercicio de potestades administrativas, a las sedes electrónicas y sedes electrónicas asociadas y sistema de firma y notificaciones electrónicas aplicables; la adhesión de los órganos constitucionales al uso de las plataformas, registros o servicios electrónicos de la Administración General del Estado; la situación de las sedes electrónicas y subsedes electrónicas en el ámbito estatal existentes a

la entrada en vigor de este real decreto; la interoperabilidad de los registros electrónicos de apoderamientos; supletoriedad en Registro Civil; la autorización de los sistemas de identificación previstos en el artículo 9.2.c) y de los sistemas de firma previstos en el artículo 10.2.c) de la Ley 39/2015, de 1 de octubre y, por último, las especialidades por razón de materia.

El Reglamento concluye con un Anexo terminológico que retoma la buena praxis que incluía la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, en una materia de especial complejidad por la imbricación de categorías jurídicas y conceptos tecnológicos en permanente evolución.

El real decreto se ajusta a los principios de buena regulación contenidos en el artículo 129 de la Ley 39/2015, de 1 de octubre (principios de necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia y eficiencia), en tanto que persigue un interés general al concretar determinados aspectos de la Ley 39/2015, de 1 de octubre y de la Ley 40/2015, de 1 de octubre, que van a facilitar el uso efectivo de los medios electrónicos de la Administración, y el desarrollo necesario de las citadas leyes. La norma es acorde con el principio de proporcionalidad al contener la regulación imprescindible para la consecución de los objetivos previamente mencionados. Igualmente, se ajusta al principio de seguridad jurídica, siendo coherente con el resto del ordenamiento jurídico, estableciéndose un marco normativo estable, integrado y claro. Asimismo, durante el procedimiento de elaboración de la norma, se han formalizado los trámites de consulta pública previa e información pública, que establece la Ley en cumplimiento del principio de transparencia, quedando además justificados en el preámbulo los objetivos que persigue este real decreto. Por último, en virtud del principio de eficiencia la norma no introduce ninguna variación, en materia de cargas administrativas, respecto de las leyes que con esta norma se desarrollan.

Asimismo, el proyecto ha sido informado por la Agencia Española de Protección de Datos y se ha sometido a consulta a las comunidades autónomas y a la Federación Española de Municipios y Provincias a través de la Comisión Sectorial de Administración Electrónica y a informe de los diferentes ministerios.

El real decreto se dicta en ejercicio de la habilitación normativa contenida en la disposición final sexta de la Ley 39/2015, de 1 de octubre, y en la disposición final decimoquinta de la Ley 40/2015, de 1 de octubre, para llevar a cabo su desarrollo reglamentario en lo referido a la gestión electrónica de los procedimientos y el funcionamiento electrónico del sector público y garantizar, así, la efectiva aplicación e implantación de las previsiones que ambas leyes establecen, todo ello al amparo de lo dispuesto en el artículo 149.1.18.ª de la Constitución. Los artículos 15,16, 23, 26, 28.2, 28.3 y 29.4 y la disposición adicional tercera del Reglamento, en cuanto a su relación con la ciberseguridad y su impacto en la seguridad de las redes y sistemas de información se dictan, además, de acuerdo con lo dispuesto en los artículos 149.1.21.ª y 149.1.29.ª de la Constitución, que atribuyen al Estado la competencia exclusiva en materia de telecomunicaciones y en materia de seguridad pública, respectivamente.

En su virtud, a propuesta de la Ministra de Asuntos Económicos y Transformación Digital y del Ministro de Política Territorial y Función Pública, de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros en su reunión del día 30 de marzo de 2021,

DISPONGO:

Artículo único. *Aprobación del Reglamento de actuación y funcionamiento del sector público por medios electrónicos.*

Se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos, cuyo texto se incluye a continuación.

Disposición transitoria primera. *Destrucción de documentos en soporte no electrónico.*

(Anulada)

Disposición transitoria segunda. *Portales de internet existentes y aplicaciones específicas en el ámbito estatal.*

1. La supresión de los portales de internet creados en el ámbito estatal antes de la entrada en vigor de este real decreto se regirá por las reglas aplicables en el momento de su creación.

2. En el plazo de seis meses desde la entrada en vigor de este real decreto, en el ámbito de cada ministerio se analizará la oportunidad del mantenimiento de sus portales de internet existentes y los de sus organismos públicos o entidades de derecho público vinculados o dependientes respectivos, así como de las páginas web promocionales («microsites»). Para ese análisis se aplicarán los mismos criterios previstos en el artículo 6 para la creación de nuevos portales y se decidirá acerca de su mantenimiento o su supresión.

En caso de que se decida la supresión, se valorará si es pertinente o no incorporar en el PAGe de la Administración General del Estado la información que se ha contenido en dichos portales hasta la supresión.

3. Realizado el proceso previsto en el apartado anterior, en el plazo máximo de un año desde la entrada en vigor de este real decreto se publicará en el PAGe de la Administración General del Estado una Resolución del Secretario General de Función Pública, en la que figurará el listado de portales de internet activos de la Administración General del Estado y de los organismos públicos o entidades de derecho público vinculados o dependientes de esta.

4. En el plazo máximo de un año desde la entrada en vigor de este real decreto, y a partir de la información facilitada por los ministerios, la Secretaría General de Administración Digital realizará el censo de aplicaciones específicas diseñadas para dispositivos móviles («app») para su utilización en los procedimientos de la Administración General del Estado.

5. En el ámbito de la Administración General del Estado, los portales de internet muy reconocidos e identificables por los usuarios, creados antes de la entrada en vigor de este real decreto se regirán por las reglas aplicables en el momento de su creación en cuanto a nomenclatura, sin necesidad de que modifiquen el nombre del dominio de segundo nivel.

Disposición derogatoria única. *Derogación normativa.*

Quedan derogadas las disposiciones de igual o inferior rango que se opongan a lo dispuesto en este real decreto y, en concreto, el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

Disposición final primera. *Títulos competenciales.*

1. Este real decreto se dicta al amparo de lo dispuesto en el artículo 149.1.18.ª de la Constitución Española, que atribuye al Estado la competencia exclusiva en materia de procedimiento administrativo común y para dictar las bases del régimen jurídico de las Administraciones Públicas.

2. Los artículos 15, 16, 23, 26, 28.2, 28.3 y 29.4 y la disposición adicional tercera del Reglamento que aprueba este real decreto, en cuanto a su relación con la ciberseguridad y su impacto en la seguridad de las redes y sistemas de información se dictan, además, de acuerdo con lo dispuesto en los artículos 149.1.21.ª y 149.1.29.ª de la Constitución, que atribuyen al Estado la competencia exclusiva en materia de telecomunicaciones y en materia de seguridad pública, respectivamente.

3. No tiene carácter básico y será de aplicación únicamente en el ámbito estatal lo dispuesto en:

a) La disposición transitoria segunda y la disposición final tercera de este real decreto.

b) El segundo párrafo del apartado 3 del artículo 3, los artículos 6, 7.4, 8, 10.3, 10.4, 13.2, 17, 18.2, 19.3, 19.4, 21.4, 23.2, 24, 25.4, 28.3, 30.2, 31, 33, 36, 38.1, el segundo párrafo del apartado 4 del artículo 39, los artículos 40, 42.5, 48, 53.5, 55.2, 57, 60.3, 62.2 y las disposiciones adicionales primera, segunda, cuarta, quinta, sexta, el segundo apartado de la disposición adicional séptima del Reglamento que aprueba este real decreto.

Disposición final segunda. *Modificación del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.*

El Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica queda modificado como sigue:

Uno. El artículo 9 queda redactado del siguiente modo:

«Artículo 9. *Inventarios de información administrativa.*

1. Cada Administración Pública mantendrá actualizado el conjunto de sus inventarios de información administrativa que incluirá, al menos:

a) La relación de los procedimientos administrativos y servicios prestados de forma clasificada y estructurada. Las Administraciones Públicas conectarán electrónicamente sus inventarios con el Sistema de Información Administrativa gestionado por el Ministerio de Política Territorial y Función Pública en colaboración con el Ministerio de Asuntos Económicos y Transformación Digital.

b) La relación de sus órganos administrativos y oficinas orientadas al público y sus relaciones entre ellos. Dicho inventario se conectará electrónicamente con el Directorio Común de Unidades Orgánicas y Oficinas, gestionado por el Ministerio de Asuntos Económicos y Transformación Digital, en colaboración con el Ministerio de Política Territorial y Función Pública, que proveerá una codificación unívoca.

2. Cada Administración Pública regulará la creación y mantenimiento de estos dos inventarios, en las condiciones que se determinen, con carácter general, por las normas técnicas de interoperabilidad correspondientes; en su caso, las Administraciones Públicas podrán hacer uso de los citados Sistema de Información Administrativa y Directorio Común de Unidades Orgánicas y Oficinas para la creación y mantenimiento de sus propios inventarios. Para la descripción y modelización de los procedimientos administrativos y de los procesos que los soportan será de aplicación lo previsto sobre estándares en el artículo 11.»

Dos. El párrafo a) del artículo 11.3, queda redactado como sigue:

«a) El uso de las especificaciones técnicas de las TIC en la contratación pública junto con las definiciones de norma y especificación técnica establecidos en el Reglamento n.º 1025/2012, del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, sobre normalización europea.»

Tres. Se modifica el artículo 14, que queda redactado como sigue:

«Artículo 14. *Plan de direccionamiento de la Administración.*

Las Administraciones Públicas aplicarán el Plan de direccionamiento e interconexión de redes en la Administración, desarrollado en la norma técnica de interoperabilidad correspondiente, para su interconexión a través de las redes de comunicaciones.»

Cuatro. Se modifica el artículo 16, que queda redactado como sigue:

«Artículo 16. *Condiciones de licenciamiento aplicables.*

1. Las condiciones de licenciamiento de las aplicaciones informáticas, documentación asociada, y cualquier otro objeto de información cuya titularidad de los derechos de la propiedad intelectual sea de una Administración Pública y permita su puesta a disposición de otra Administración y de los ciudadanos tendrán en cuenta los siguientes aspectos:

a) El fin perseguido es el aprovechamiento y la reutilización de recursos públicos.

b) La completa protección contra su apropiación exclusiva o parcial por parte de terceros.

c) La exención de responsabilidad del cedente por el posible mal uso por parte del cesionario.

d) La no obligación de asistencia técnica o de mantenimiento por parte del cedente.

e) La ausencia total de responsabilidad por parte del cedente con respecto al cesionario en caso de errores o mal funcionamiento de la aplicación.

f) El licenciamiento se realizará por defecto sin contraprestación y sin necesidad de establecer convenio alguno. Sólo se podrá acordar la repercusión parcial del coste de adquisición o desarrollo de las aplicaciones cedidas en aquellos casos en los que este pago repercuta directamente en el incremento de funcionalidades del activo cedido, incluya adaptaciones concretas para su uso en el organismo cesionario, o impliquen el suministro de servicios de asistencia o soporte para su reutilización en el organismo cesionario.

2. Las Administraciones Públicas utilizarán para las aplicaciones informáticas, documentación asociada, y cualquier otro objeto de información declarados como de fuentes abiertas aquellas licencias que aseguren que los programas, datos o información cumplen los siguientes requisitos:

a) Pueden ejecutarse para cualquier propósito.

b) Permiten conocer su código fuente.

c) Pueden modificarse o mejorarse.

d) Pueden redistribuirse a otros usuarios con o sin cambios siempre que la obra derivada mantenga estas cuatro garantías.

3. Para este fin se procurará la aplicación de la Licencia Pública de la Unión Europea, sin perjuicio de otras licencias que garanticen los mismos derechos expuestos en los apartados 1 y 2.

4. A efectos de facilitar el establecimiento de las condiciones de licenciamiento, las Administraciones Públicas incluirán en los pliegos de cláusulas técnicas de aquellos contratos que tengan por finalidad el desarrollo de nuevas aplicaciones informáticas, los siguientes aspectos:

a) Que la Administración contratante adquiera los derechos completos de propiedad intelectual de las aplicaciones y cualquier otro objeto de información que se desarrollen como objeto de ese contrato.

b) Que en el caso de reutilizar activos previamente existentes, la Administración contratante reciba un producto que pueda ofrecer para su reutilización posterior a otras Administraciones Públicas. Además, en el caso de partir de productos de fuentes abiertas, que sea posible declarar como de fuentes abiertas la futura aplicación desarrollada.»

Cinco. Se modifica el artículo 17, que queda redactado como sigue:

«Artículo 17. *Directorios de aplicaciones reutilizables.*

1. La Administración General del Estado mantendrá el Directorio general de aplicaciones para su libre reutilización, de acuerdo al artículo 158 de la Ley 40/2015, de 1 octubre, a través del Centro de Transferencia de Tecnología. Este directorio podrá ser utilizado por otras Administraciones Públicas. En el caso de disponer de un directorio propio, deberá garantizar que las aplicaciones disponibles en ese directorio propio se pueden consultar también a través del Centro de Transferencia de Tecnología.

2. Las Administraciones Públicas conectarán los directorios de aplicaciones para su libre reutilización entre sí; y con instrumentos equivalentes del ámbito de la Unión Europea.

3. Las Administraciones Públicas publicarán las aplicaciones reutilizables, en modo producto o en modo servicio, en los directorios de aplicaciones para su libre reutilización, con al menos el siguiente contenido:

a) Código fuente de las aplicaciones finalizadas, en el caso de ser reutilizables en modo producto y haber sido declaradas de fuentes abiertas.

b) Documentación asociada.

c) Condiciones de licenciamiento de todos los activos, en el caso de ser reutilizables en modo producto, o nivel de servicio ofrecido, en el caso de ser reutilizables en modo servicio.

d) Los costes asociados a su reutilización, en el caso de que existieran.

4. Las Administraciones procurarán la incorporación a la aplicación original de aquellas modificaciones o adaptaciones realizadas sobre cualquier aplicación que se haya obtenido desde un directorio de aplicaciones reutilizables.»

Seis. Se modifica el artículo 18, que queda redactado como sigue:

«Artículo 18. *Interoperabilidad en la política de firma electrónica y de certificados.*

1. La Administración General del Estado definirá una política de firma electrónica y de certificados que servirá de marco general de interoperabilidad para el reconocimiento mutuo de las firmas electrónicas basadas en certificados de documentos administrativos en las Administraciones Públicas.

Todos los organismos y entidades de derecho público de la Administración General del Estado aplicarán la política de firma electrónica y de certificados a que se refiere el párrafo anterior. La no aplicación de dicha política deberá ser justificada por el órgano u organismo competente y autorizada por la Secretaría General de Administración Digital.

2. Las restantes Administraciones Públicas podrán acogerse a la política de firma electrónica y de certificados a que hace referencia el apartado anterior.

3. Sin perjuicio de lo expuesto en el apartado anterior, las Administraciones Públicas podrán aprobar otras políticas de firma electrónica dentro de sus respectivos ámbitos competenciales.

Las políticas de firma electrónica que aprueben las Administraciones Públicas partirán de la norma técnica establecida a tal efecto en la disposición adicional primera, de los estándares técnicos existentes, y deberán ser interoperables con la política marco de firma electrónica mencionada en el apartado 1, en particular, con sus ficheros de implementación. La Administración Pública proponente de una política de firma electrónica particular garantizará su interoperabilidad con la citada política marco de firma electrónica y con sus correspondientes ficheros de implementación según las condiciones establecidas en la norma técnica de interoperabilidad recogida a tal efecto en la disposición adicional primera.

4. Al objeto de garantizar la interoperabilidad de las firmas electrónicas emitidas conforme a las políticas establecidas, las políticas de firma electrónica que las Administraciones Públicas aprueben deberán ser comunicadas, junto con sus correspondientes ficheros de implementación, a la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital.

5. Las Administraciones Públicas receptoras de documentos electrónicos firmados, siempre que hayan admitido con anterioridad la política de firma del emisor, permitirán la validación de las firmas electrónicas según la política de firma indicada en la firma del documento electrónico.

6. Los perfiles comunes de los campos de los certificados definidos por la política de firma electrónica y de certificados posibilitarán la interoperabilidad entre las aplicaciones usuarias, de manera que tanto la identificación como la firma electrónica generada a partir de estos perfiles comunes puedan ser reconocidos por las aplicaciones de las distintas Administraciones Públicas sin ningún tipo de restricción técnica, semántica u organizativa.

7. Los procedimientos en los que se utilicen certificados de firma electrónica deberán atenerse a la política de firma electrónica y de certificados aplicable en su ámbito, particularmente en la aplicación de los datos obligatorios y opcionales, las

reglas de creación y validación de firma electrónica, los algoritmos a utilizar y longitudes de clave mínimas aplicables.»

Siete. Se elimina el artículo 19.
Ocho. Se modifica la disposición adicional primera, que queda redactada como sigue:

«Disposición adicional primera. *Desarrollo del Esquema Nacional de Interoperabilidad.*

1. Se desarrollarán las siguientes normas técnicas de interoperabilidad que serán de obligado cumplimiento por parte de las Administraciones Públicas:

a) Norma Técnica de Catálogo de estándares: establecerá un conjunto de estándares que satisfagan lo previsto en el artículo 11 de forma estructurada y con indicación de los criterios de selección y ciclo de vida aplicados.
b) Norma Técnica de Documento electrónico: tratará los metadatos mínimos obligatorios, la asociación de los datos y metadatos de firma o de sellado de tiempo, así como otros metadatos complementarios asociados; y los formatos de documento.
c) Norma Técnica de Digitalización de documentos: tratará los formatos y estándares aplicables, los niveles de calidad, las condiciones técnicas y los metadatos asociados al proceso de digitalización.
d) Norma Técnica de Expediente electrónico: tratará de su estructura y formato, así como de las especificaciones de los servicios de remisión y puesta a disposición.
e) Norma Técnica de Política de firma electrónica y de certificados de la Administración: Tratará, entre otras cuestiones recogidas en su definición en el anexo, aquellas que afectan a la interoperabilidad incluyendo los formatos de firma, los algoritmos a utilizar y longitudes mínimas de las claves, las reglas de creación y validación de la firma electrónica, la gestión de las políticas de firma, el uso de las referencias temporales y de sello de tiempo, así como la normalización de la representación de la firma electrónica en pantalla y en papel para el ciudadano y en las relaciones entre las Administraciones Públicas.
f) Norma Técnica de Protocolos de intermediación de datos: tratará las especificaciones de los protocolos de intermediación de datos que faciliten la integración y reutilización de servicios en las Administraciones Públicas y que serán de aplicación para los prestadores y consumidores de tales servicios.
g) Norma Técnica de Relación de modelos de datos que tengan el carácter de comunes en la Administración y aquellos que se refieran a materias sujetas a intercambio de información con los ciudadanos y otras Administraciones.
h) Norma Técnica de Política de gestión de documentos electrónicos: incluirá directrices para la asignación de responsabilidades, tanto directivas como profesionales, y la definición de los programas, procesos y controles de gestión de documentos y administración de los repositorios electrónicos, y la documentación de los mismos, a desarrollar por las Administraciones Públicas y por los organismos públicos y entidades de derecho público vinculados o dependientes de aquéllas.
i) Norma Técnica de Requisitos de conexión a la Red de comunicaciones de las Administraciones Públicas españolas.
j) Norma Técnica de Procedimientos de copiado auténtico y conversión entre documentos electrónicos, así como desde papel u otros medios físicos a formatos electrónicos.
k) Norma Técnica de Modelo de Datos para el intercambio de asientos entre las Entidades Registrales: tratará de aspectos funcionales y técnicos para el intercambio de asientos registrales, gestión de errores y excepciones, gestión de anexos, requerimientos tecnológicos y transformaciones de formatos.
l) Norma Técnica de Reutilización de recursos de información: tratará de las normas comunes sobre la localización, descripción e identificación unívoca de los recursos de información puestos a disposición del público por medios electrónicos para su reutilización.
m) Norma Técnica de interoperabilidad de inventario y codificación de objetos administrativos: tratará las reglas relativas a la codificación de objetos

administrativos, así como la conexión entre los inventarios correspondientes, incluyendo, por un lado, las unidades orgánicas y oficinas de la Administración, y, por otro lado, la información administrativa de procedimientos y servicios.

n) Norma Técnica de Interoperabilidad de Transferencia e Ingreso de documentos y expedientes electrónicos: tratará los requisitos y condiciones relativos a la transferencia de agrupaciones documentales en formato electrónico, documentos y expedientes electrónicos, junto con los metadatos asociados, entre sistemas de gestión de documentos electrónicos y sistemas de archivo electrónico.

ñ) Norma Técnica de Interoperabilidad de Valoración y Eliminación de documentos y expedientes electrónicos: tratará las condiciones y requisitos relativos a la valoración de los documentos y expedientes electrónicos para establecimiento de plazos de conservación, transferencia y acceso o, en su caso, eliminación total o parcial.

o) Norma Técnica de Interoperabilidad de preservación de documentación electrónica: tratará las condiciones y requisitos relativos a la conservación de los documentos electrónicos para garantizar su autenticidad, integridad, confidencialidad, disponibilidad y trazabilidad, así como la protección, recuperación y conservación física y lógica de los documentos y su contexto.

p) Norma Técnica de Interoperabilidad de tratamiento y preservación de bases de datos: tratará las condiciones y requisitos relativos a la conservación de las bases de datos para garantizar su autenticidad, integridad, confidencialidad, disponibilidad y trazabilidad, y permitiendo la protección, recuperación y conservación física y lógica de los datos y su contexto.

q) Norma Técnica de Interoperabilidad de Plan de Direccionamiento: tratará reglas aplicables a la asignación y requisitos de direccionamiento IP para garantizar la correcta administración de la Red de comunicaciones de las Administraciones Públicas españolas y evitar el uso de direcciones duplicadas.

r) Norma Técnica de Interoperabilidad de reutilización de activos en modo producto y en modo servicio: tratará los requisitos y condiciones para facilitar la reutilización de activos tanto en modo producto como en modo servicio por las Administraciones Públicas españolas.

s) Norma Técnica de Interoperabilidad del modelo de datos y condiciones de interoperabilidad de los registros de funcionarios habilitados: tratará los aspectos funcionales y técnicos para la plena interoperabilidad de los registros electrónicos de funcionarios habilitados pertenecientes a las Administraciones, así como la interconexión de estos a las sedes electrónicas.

t) Norma Técnica de Interoperabilidad del modelo de datos y condiciones de interoperabilidad de los registros electrónicos de apoderamientos: tratará los aspectos funcionales y técnicos para la plena interoperabilidad de los registros electrónicos de apoderamientos pertenecientes a las Administraciones, así como la interconexión de estos a las sedes electrónicas, A los registros mercantiles, de la propiedad, y a los protocolos notariales.

u) Norma Técnica de Interoperabilidad de Sistema de Referencia de documentos y repositorios de confianza: tratará los requisitos técnicos que deberán cumplir las referencias a documentos al ser intercambiadas, de forma que se evite trasladar documentación de forma innecesaria.

v) Norma Técnica de Política de firma electrónica y de certificados en el ámbito estatal: tratará las directrices y normas técnicas aplicables a la utilización de certificados y firma electrónica dentro de su ámbito de aplicación, organizadas alrededor de los conceptos de generación y validación de firma e incluirá los perfiles interoperables de los medios de identificación de las Administraciones Públicas previstos en Ley 40/2015, de 1 de octubre.

2. El Ministerio de Asuntos Económicos y Transformación Digital, a propuesta de la Comisión Sectorial de Administración Electrónica prevista en la disposición adicional novena de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, aprobará las normas técnicas de interoperabilidad y las publicará mediante Resolución de la Secretaria de Estado de Digitalización e Inteligencia Artificial.

3. Para la redacción y actualización de las normas técnicas de interoperabilidad indicadas en el apartado 1 y las futuras que pueda aprobar el Ministerio de Asuntos Económicos y Transformación Digital que sean necesarias para garantizar el adecuado nivel de interoperabilidad como consecuencia del nivel de desarrollo tecnológico, los compromisos internacionales o el marco normativo aplicable, se constituirán los correspondientes grupos de trabajo en los órganos colegiados con competencias en materia de Administración electrónica.

Para garantizar la debida interoperabilidad en materia de ciberseguridad y criptografía, en relación con la aplicación del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la administración electrónica, el órgano competente será el Centro Criptológico Nacional, adscrito al Centro Nacional de Inteligencia.

4. Se desarrollarán los siguientes instrumentos para la interoperabilidad:

a) Sistema de Información Administrativa: Inventario de procedimientos administrativos, servicios prestados y otras actuaciones administrativas que generen documentación pública, conteniendo información de los mismos clasificada por funciones y con indicación de su nivel de informatización, así como información acerca de las interfaces al objeto de favorecer la interacción o en su caso la integración de los procesos.

b) Centro de interoperabilidad semántica de la Administración: Almacenará, publicará y difundirá los modelos de datos de los servicios de interoperabilidad entre Administraciones Públicas y de estas con los ciudadanos, tanto comunes como sectoriales, así como los relativos a infraestructuras y servicios comunes, además de las especificaciones semánticas y codificaciones relacionadas. Su propósito es facilitar la comprensión semántica de los servicios de intercambio de datos de las Administraciones y maximizar la reutilización de activos semánticos en la construcción de éstos. Se conectará con otros instrumentos equivalentes de las Administraciones Públicas y del ámbito de la Unión Europea.

c) Centro de Transferencia de Tecnología: Directorio de aplicaciones para su libre reutilización que contendrá la relación de aplicaciones para su libre reutilización, incluyendo, al menos, los datos descriptivos relativos a nombre de la aplicación, breve descripción de sus funcionalidades, uso y características, licencia, principales estándares abiertos aplicados, y estado de desarrollo.

d) Directorio Común de Unidades Orgánicas y Oficinas de las Administraciones Públicas: Instrumento que permitirá la sincronización de los sistemas que traten la información de inventariado, codificación y evolución de unidades orgánicas y oficinas en diferentes modalidades de integración para garantizar la flexibilidad tanto en el consumo como en la provisión de información relacionada.»

Nueve. Se suprime la disposición adicional tercera.

Diez. Se suprime la disposición adicional cuarta.

Once. Se modifica el anexo de la forma siguiente:

1. Se suprime el término « Familia».

2. A continuación del término «Índice electrónico» se sustituye el vigente término «Infraestructuras y servicios comunes» por el término «Infraestructura o servicio común» con la siguiente redacción:

«Infraestructura o servicio común: capacidad organizativa y técnica que satisface necesidades comunes de los usuarios en diversos ámbitos de la Administración, junto con su gobernanza operativa de apoyo, que pueden tener carácter horizontal o sectorial, con diversos modos de provisión, como servicio o como producto, o integración a modo de plataforma, que facilitan la interoperabilidad, la seguridad, las economías de escala, la racionalización y la simplificación de la actuación administrativa.»

3. A continuación del término «Estándar abierto» se introduce el término «Ficheros de implementación de las políticas de firma« con la siguiente redacción:

«Ficheros de implementación de las políticas de firma: Son la representación en lenguaje formal (XML o ASN.1) de las condiciones establecidas en la política de firma, acorde a las normas técnicas establecidas por los organismos de estandarización.»

Disposición final tercera. *Modificación del Real Decreto 931/2017, de 27 de octubre, por el que se regula la Memoria del Análisis de Impacto Normativo.*

Se modifican el párrafo segundo de la letra d) y la letra g) del apartado 1 del artículo 2 del Real Decreto 931/2017, de 27 de octubre, por el que se regula la Memoria del Análisis de Impacto Normativo, que quedan redactados como sigue:

«2.º El Impacto presupuestario comprenderá, al menos, una referencia a los efectos en los ingresos y gastos públicos e incluirá la incidencia en los gastos de personal, dotaciones o retribuciones, gastos en medios o servicios de la Administración digital o cualesquiera otros gastos al servicio del sector público.»

«g) Otros impactos: La memoria del análisis de impacto normativo incluirá cualquier otro extremo que pudiera ser relevante a criterio del órgano proponente, prestando especial atención a los impactos de carácter social y medioambiental, al impacto en materia de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad y al impacto que tendrá para la ciudadanía y para la Administración el desarrollo o uso de los medios y servicios de la Administración digital que conlleve la norma.»

Disposición final cuarta. *Habilitación normativa.*

Se faculta a la persona titular del Ministerio de Política Territorial y Función Pública y a la persona titular del Ministerio de Asuntos Económicos y Transformación Digital en el ámbito de sus competencias, para dictar las disposiciones y adoptar las medidas necesarias para el desarrollo y ejecución de este real decreto y del Reglamento que aprueba, así como para modificar el anexo del mismo.

Disposición final quinta. *Entrada en vigor.*

Este real decreto entrará en vigor el día 2 de abril de 2021.

REGLAMENTO DE ACTUACIÓN Y FUNCIONAMIENTO DEL SECTOR PÚBLICO POR MEDIOS ELECTRÓNICOS

TÍTULO PRELIMINAR

Disposiciones generales

Artículo 1. *Objeto y ámbito de aplicación.*

1. Este Reglamento tiene por objeto el desarrollo de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en lo referido a la actuación y el funcionamiento electrónico del sector público.
2. El ámbito subjetivo de aplicación es el establecido en el artículo 2 de la Ley 39/2015, de 1 de octubre, y el artículo 2 de la Ley 40/2015, de 1 de octubre.

Artículo 2. *Principios generales.*

El sector público deberá respetar los siguientes principios en sus actuaciones y relaciones electrónicas:

a) Los principios de neutralidad tecnológica y de adaptabilidad al progreso de las tecnologías y sistemas de comunicaciones electrónicas, para garantizar tanto la independencia en la elección de las alternativas tecnológicas necesarias para relacionarse

con las Administraciones Públicas por parte de las personas interesadas y por el propio sector público, como la libertad para desarrollar e implantar los avances tecnológicos en un ámbito de libre mercado. A estos efectos, el sector público utilizará estándares abiertos, así como, en su caso y de forma complementaria, estándares que sean de uso generalizado.

Las herramientas y dispositivos que deban utilizarse para la comunicación por medios electrónicos, así como sus características técnicas, serán no discriminatorios, estarán disponibles de forma general y serán compatibles con los productos informáticos de uso general.

b) El principio de accesibilidad, entendido como el conjunto de principios y técnicas que se deben respetar al diseñar, construir, mantener y actualizar los servicios electrónicos para garantizar la igualdad y la no discriminación en el acceso de las personas usuarias, en particular de las personas con discapacidad y de las personas mayores.

c) El principio de facilidad de uso, que determina que el diseño de los servicios electrónicos esté centrado en las personas usuarias, de forma que se minimice el grado de conocimiento necesario para el uso del servicio.

d) El principio de interoperabilidad, entendido como la capacidad de los sistemas de información y, por ende, de los procedimientos a los que éstos dan soporte, de compartir datos y posibilitar el intercambio de información entre ellos.

e) El principio de proporcionalidad, en cuya virtud sólo se exigirán las garantías y medidas de seguridad adecuadas a la naturaleza y circunstancias de los distintos trámites y actuaciones electrónicos.

f) El principio de personalización y proactividad, entendido como la capacidad de las Administraciones Públicas para que, partiendo del conocimiento adquirido del usuario final del servicio, proporcione servicios precumplimentados y se anticipe a las posibles necesidades de los mismos.

Artículo 3. *Derecho y obligación de relacionarse electrónicamente con las Administraciones Públicas.*

1. Estarán obligados a relacionarse a través de medios electrónicos con las Administraciones Públicas para la realización de cualquier trámite de un procedimiento administrativo, al menos, los sujetos a los que se refiere el artículo 14.2 de la Ley 39/2015, de 1 de octubre.

2. Las personas físicas no obligadas a relacionarse a través de medios electrónicos con las Administraciones Públicas podrán ejercitar su derecho a relacionarse electrónicamente con la Administración Pública de que se trate al inicio del procedimiento y, a tal efecto, lo comunicarán al órgano competente para la tramitación del mismo de forma que este pueda tener constancia de dicha decisión. La voluntad de relacionarse electrónicamente o, en su caso, de dejar de hacerlo cuando ya se había optado anteriormente por ello, podrá realizarse en una fase posterior del procedimiento, si bien deberá comunicarse a dicho órgano de forma que quede constancia de la misma. En ambos casos, los efectos de la comunicación se producirán a partir del quinto día hábil siguiente a aquel en que el órgano competente para tramitar el procedimiento haya tenido constancia de la misma.

3. De acuerdo con lo previsto en el apartado 3 del artículo 14 de la Ley 39/2015, de 1 de octubre, la obligatoriedad de relacionarse electrónicamente podrá establecerse reglamentariamente por las Administraciones Públicas para determinados procedimientos y para ciertos colectivos de personas físicas que, por razón de su capacidad económica, técnica, dedicación profesional u otros motivos, quede acreditado que tienen acceso y disponibilidad de los medios electrónicos necesarios.

A tal efecto, en el ámbito estatal la mencionada obligatoriedad de relacionarse por medios electrónicos con sus órganos, organismos y entidades de derecho público podrá ser establecida por real decreto acordado en Consejo de Ministros o por orden de la persona titular del Departamento competente respecto de los procedimientos de que se trate que afecten al ámbito competencial de uno o varios Ministerios cuya regulación no requiera de norma con rango de real decreto. Asimismo, se publicará en el Punto de Acceso General electrónico (PAGe) de la Administración General del Estado y en la sede electrónica o sede asociada que corresponda.

Artículo 4. *Canales de asistencia para el acceso a los servicios electrónicos.*

Las Administraciones Públicas prestarán la asistencia necesaria para facilitar el acceso de las personas interesadas a los servicios electrónicos proporcionados en su ámbito competencial a través de alguno o algunos de los siguientes canales:

a) Presencial, a través de las oficinas de asistencia que se determinen.
b) Portales de internet y sedes electrónicas.
c) Redes sociales.
d) Telefónico.
e) Correo electrónico.
f) Cualquier otro canal que pueda establecerse de acuerdo con lo previsto en el artículo 12 de la Ley 39/2015, de 1 de octubre.

TÍTULO I

Portales de internet, Punto de Acceso General electrónico y sedes electrónicas

Artículo 5. *Portales de internet de las Administraciones Públicas.*

1. De acuerdo con lo previsto en el artículo 39 de la Ley 40/2015, de 1 de octubre, se entiende por portal de internet el punto de acceso electrónico cuya titularidad corresponda a una Administración Pública, organismo público o entidad de derecho público que permite el acceso a través de internet a la información y, en su caso, a la sede electrónica o sede electrónica asociada correspondiente.

2. Cada Administración podrá determinar los contenidos y canales mínimos de atención a las personas interesadas y de difusión y prestación de servicios que deban tener sus portales, así como criterios obligatorios de imagen institucional. En cualquier caso, deberán tenerse en cuenta los contenidos, formatos y funcionalidades que en la normativa de reutilización, accesibilidad y transparencia se establezcan como obligatorios para los sitios web.

3. Los portales de internet dispondrán de sistemas que permitan el establecimiento de medidas de seguridad de acuerdo con lo establecido en Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Artículo 6. *Creación y supresión de portales de internet en el ámbito estatal.*

1. En el ámbito estatal, la creación o supresión de portales se llevará a cabo por orden de la persona titular del ministerio correspondiente o por resolución de la persona titular del órgano superior, en el caso de la Administración General del Estado, y por resolución de la persona titular de la Presidencia o de la Dirección en el caso de sus organismos públicos y entidades de derecho público vinculados o dependientes.

La creación requerirá informe favorable de la Comisión Ministerial de Administración Digital respectiva y posterior comunicación al Ministerio de Política Territorial y Función Pública y al Ministerio de Asuntos Económicos y Transformación Digital. Para obtener dicho informe favorable, la propuesta de creación del nuevo portal se deberá justificar en términos de eficiencia en la asignación y utilización de los recursos públicos e interés prioritario para la implantación de una política pública o la aplicación de la normativa de la Unión Europea o nacional y a tal efecto el órgano promotor de la creación del nuevo portal remitirá una memoria justificativa y económica.

La supresión de portales requerirá la previa comunicación al Ministerio de Política Territorial y Función Pública y al Ministerio de Asuntos Económicos y Transformación Digital.

2. El acto o resolución de creación de un nuevo portal previsto en el apartado anterior contendrá, al menos, la identificación de su dirección electrónica, que deberá incluir el nombre de dominio de segundo nivel «.gob.es», su ámbito funcional y, en su caso, orgánico y la finalidad para la que se crea. Para facilitar su identificación, seguirán las disposiciones generales que se establezcan para la imagen institucional de la Administración General del Estado.

3. En el ámbito estatal los portales de internet a los que se refiere este artículo deberán estar referenciados en el PAGe de la Administración General del Estado.

Artículo 7. *Punto de Acceso General electrónico.*

1. Las Administraciones Públicas contarán con un Punto de Acceso General electrónico (PAGe).

2. El PAGe de cada Administración Pública facilitará el acceso a los servicios, trámites e información de los órganos, organismos públicos y entidades vinculados o dependientes de la Administración Pública correspondiente.

3. El PAGe dispondrá de una sede electrónica, a través de la cual se podrá acceder a todas las sedes electrónicas y sedes asociadas de la Administración Pública correspondiente.

Además, esta sede podrá incluir un área personalizada a través de la cual cada interesado, mediante procedimientos seguros que garanticen la integridad y confidencialidad de sus datos personales, podrá acceder a su información, al seguimiento de los trámites administrativos que le afecten y a las notificaciones y comunicaciones en el ámbito de la Administración Pública competente.

4. El PAGe de la Administración General del Estado y su sede electrónica serán gestionados por el Ministerio de Política Territorial y Función Pública en colaboración con la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital.

En dicha sede electrónica está alojada la Dirección Electrónica Habilitada única a la que se refiere el artículo 43 de la Ley 39/2015, de 1 de octubre.

El PAGe de la Administración General del Estado, a través de su sede, permitirá la comprobación de la autenticidad e integridad de los documentos facilitados por el sector público estatal a través del Código Seguro de Verificación o de cualquier otro sistema de firma o sello basado en certificado electrónico cualificado que se haya utilizado en su generación. También permitirá, en su caso, su recuperación.

5. El PAGe de la Administración General del Estado podrá interoperar con portales web oficiales de la Unión Europea.

Artículo 8. *Carpeta Ciudadana del sector público estatal.*

1. La Carpeta Ciudadana es el área personalizada de las personas interesadas a que se refiere el artículo 7.3 en su relación con el sector público estatal. Además del interesado podrán acceder a la Carpeta Ciudadana:

a) Sus representantes legales.

b) Quien ostente un poder general previsto en el artículo 6.4.a) de la Ley 39/2015, de 1 de octubre, otorgado por el interesado e inscrito en el Registro Electrónico de Apoderamientos.

2. La Carpeta Ciudadana será accesible a través de la sede electrónica del PAGe de la Administración General del Estado y podrá ofrecer, entre otras, las funcionalidades siguientes para el interesado o sus representantes:

a) Permitir el seguimiento del estado de tramitación de los procedimientos en que sea interesado, de acuerdo con lo previsto en el artículo 53.1.a) de la Ley 39/ 2015, de 1 de octubre.

b) Permitir el acceso a sus comunicaciones y notificaciones.

c) Conocer qué datos suyos obran en poder del sector público estatal, sin perjuicio de las limitaciones que establezca la normativa vigente.

d) Facilitar la obtención de certificaciones administrativas exigidas por la normativa correspondiente.

3. El interesado accederá a la Carpeta Ciudadana mediante los sistemas de identificación a los que se refiere el artículo 9.2 de la Ley 39/2015, de 1 de octubre.

4. El interesado deberá asegurar el buen uso de los sistemas de identificación y velar por que el acceso a su carpeta Ciudadana solo se haga por sí mismo o por tercero autorizado.

Artículo 9. *Sedes electrónicas de las Administraciones Públicas.*

1. De acuerdo con lo previsto en el artículo 38 de la Ley 40/2015, de 1 de octubre, una sede electrónica es aquella dirección electrónica disponible para la ciudadanía por medio de redes de telecomunicaciones. Mediante dicha sede electrónica se realizarán todas las actuaciones y trámites referidos a procedimientos o a servicios que requieran la identificación de la Administración Pública y, en su caso, la identificación o firma electrónica de las personas interesadas.

2. La titularidad de la sede electrónica corresponde a una Administración Pública, o bien a uno o varios organismos públicos o entidades de derecho público en el ámbito de sus competencias.

Artículo 10. *Creación y supresión de las sedes electrónicas y sedes electrónicas asociadas.*

1. Se podrán crear una o varias sedes electrónicas asociadas a una sede electrónica atendiendo a razones técnicas y organizativas. La sede electrónica asociada tendrá consideración de sede electrónica a todos los efectos.

2. El acto o resolución de creación o supresión de una sede electrónica o sede electrónica asociada será publicado en el boletín oficial que corresponda en función de cuál sea la Administración Pública titular de la sede o sede asociada y también en el directorio del Punto de Acceso General Electrónico que corresponda. En el caso de las entidades locales, el boletín oficial será el de la provincia al que pertenezca la entidad.

El acto o resolución de creación determinará, al menos:

a) El ámbito de aplicación de la sede electrónica o sede electrónica asociada.

b) La identificación de la dirección electrónica de referencia de la sede electrónica o sede electrónica asociada que se cree, así como de las direcciones electrónicas de las sedes electrónicas que desde el momento de la creación ya sean asociadas de aquella. Las sedes electrónicas asociadas con posterioridad a la publicación del instrumento de creación se referenciarán en la mencionada dirección electrónica.

c) La identificación de su titular.

d) La identificación del órgano u órganos encargados de la gestión y de los servicios puestos a disposición en la misma.

3. En el ámbito estatal, tanto la creación o supresión de una sede electrónica asociada a la sede electrónica del PAGe de la Administración General del Estado como la creación o supresión de sedes electrónicas o sedes electrónicas asociadas de los organismos públicos y entidades de derecho público vinculados o dependientes se hará mediante orden de la persona titular del Departamento competente o por resolución de la persona titular de la Presidencia o de la Dirección del organismo o entidad de derecho público competente, con el informe previo favorable del Ministerio de Política Territorial y Función Pública y del Ministerio de Asuntos Económicos y Transformación Digital.

4. Para obtener los informes previos favorables a que se refiere el apartado anterior, la propuesta de creación de la nueva sede electrónica o, en su caso, sede electrónica asociada se tendrá que justificar, en términos de eficiencia en la asignación y utilización de recursos públicos. A tal efecto, el órgano promotor de la creación de la sede electrónica remitirá una memoria justificativa y económica en que se explicite el volumen de trámites que está previsto gestionar a través de la misma, los efectos presupuestarios y económicos de su establecimiento, su incidencia en la reducción del tiempo de resolución de los procedimientos y de cargas administrativas para las personas interesadas y cualquier otra razón de interés general que justifique su creación.

Artículo 11. *Contenido y servicios de las sedes electrónicas y sedes asociadas.*

1. Toda sede electrónica o sede electrónica asociada dispondrá del siguiente contenido mínimo a disposición de las personas interesadas:

a) La identificación de la sede electrónica o sede electrónica asociada, así como del órgano u organismo titular de la misma y los órganos competentes para la gestión de la información, servicios, procedimientos y trámites puestos a disposición en ella.

b) La identificación del acto o disposición de creación y el acceso al mismo, directamente o mediante enlace a su publicación en el Boletín Oficial correspondiente.

c) La información necesaria para la correcta utilización de la sede electrónica, incluyendo su mapa o información equivalente, con especificación de la estructura de navegación y las distintas secciones disponibles, así como la relativa a propiedad intelectual, protección de datos personales y accesibilidad.

d) La relación de sistemas de identificación y firma electrónica que sean admitidos o utilizados en la misma.

e) La normativa reguladora del Registro al que se acceda a través de la sede electrónica.

f) La fecha y hora oficial, así como el calendario de días inhábiles a efectos del cómputo de plazos aplicable a la Administración en que se integre el órgano, organismo público o entidad de derecho público vinculado o dependiente que sea titular de la sede electrónica o sede electrónica asociada.

g) Información acerca de cualquier incidencia técnica que acontezca e imposibilite el funcionamiento ordinario del sistema o aplicación que corresponda, así como de la ampliación del plazo no vencido que, en su caso, haya acordado el órgano competente debido a dicha circunstancia.

h) Relación actualizada de los servicios, procedimientos y trámites disponibles

i) Relación actualizada de las actuaciones administrativas automatizadas vinculadas a los servicios, procedimientos y trámites descritos en la letra anterior. Cada una se acompañará de la descripción de su diseño y funcionamiento, los mecanismos de rendición de cuentas y transparencia, así como los datos utilizados en su configuración y aprendizaje.

2. Las sedes electrónicas y sedes electrónicas asociadas dispondrán, al menos, de los siguientes servicios a disposición de las personas interesadas:

a) Un acceso a los servicios y trámites disponibles en la sede electrónica o sede electrónica asociada, con indicación de los plazos máximos de duración de los procedimientos, excluyendo las posibles ampliaciones o suspensiones que en su caso, pudiera acordar el órgano competente.

b) Un enlace para la formulación de sugerencias y quejas ante los órganos que en cada caso resulten competentes.

c) Los mecanismos de comunicación y procedimiento de reclamación establecidos al respecto de los requisitos de accesibilidad de los sitios web y aplicaciones móviles del sector público.

d) Un sistema de verificación de los certificados de la sede electrónica.

e) Un sistema de verificación de los sellos electrónicos de los órganos, organismos públicos o entidades de derecho público que abarque la sede electrónica o sede electrónica asociada.

f) Un servicio de comprobación de la autenticidad e integridad de los documentos emitidos por los órganos, organismos públicos o entidades de derecho público comprendidos en el ámbito de la sede electrónica, que hayan sido firmados por cualquiera de los sistemas de firma conformes a la Ley 40/2015, 1 de octubre, y para los cuales se haya generado un código seguro de verificación.

g) Un acceso a los modelos, y sistemas de presentación masiva, de uso voluntario, que permitan a las personas interesadas presentar simultáneamente varias solicitudes en la forma que establezca, en su caso, cada Administración, organismo público o entidad de derecho público titular de la sede electrónica o sede electrónica asociada.

h) El acceso a los modelos normalizados de presentación de solicitudes que establezca, en su caso, cada Administración u organismo público o entidad de derecho público titular de la sede electrónica o sede electrónica asociada.

i) Un servicio de consulta del directorio geográfico de oficinas de asistencia en materia de registros, que permita al interesado identificar la más próxima a su dirección de consulta.

3. De acuerdo con lo previsto en el artículo 66.1 de la Ley 39/2015, de 1 de octubre, las Administraciones Públicas deberán mantener y actualizar en la sede electrónica correspondiente un listado con los códigos de identificación vigentes de sus órganos, centros o unidades administrativas.

Artículo 12. *Responsabilidad sobre la sede electrónica o sede electrónica asociada.*

1. El titular de la sede electrónica y, en su caso, de la sede electrónica asociada, será responsable de la integridad, veracidad y actualización de la información y los servicios de su competencia a los que pueda accederse a través de la misma.

2. En caso de que la sede electrónica o sede electrónica asociada contenga un enlace o vínculo a otra sede o sede asociada, será el titular de esta última el responsable de la integridad, veracidad y actualización de la información o procedimientos que figuren en la misma, sin perjuicio de la debida diligencia del titular de la primera respecto de la incorporación de los contenidos en la misma.

3. En caso de que una sede electrónica o sede electrónica asociada contenga procedimientos, servicios o ambos, cuya competencia corresponda a otro órgano administrativo, organismo público o entidad de derecho público vinculado o dependiente, sea de la misma o de diferente Administración, el titular de la competencia será responsable de la integridad, veracidad y actualización de lo relativo a dichos procedimientos, servicios o ambos sin perjuicio de la debida diligencia del titular de la sede electrónica o sede electrónica asociada respecto de la incorporación de los contenidos en la misma.

TÍTULO II

Procedimiento administrativo por medios electrónicos

CAPÍTULO I

Disposiciones generales

Artículo 13. *Actuación administrativa automatizada.*

1. La tramitación electrónica de una actuación administrativa podrá llevarse a cabo, entre otras formas, de manera automatizada de acuerdo con lo previsto en el artículo 41 de la Ley 40/2015, de 1 de octubre.

2. En el ámbito estatal la determinación de una actuación administrativa como automatizada se autorizará por resolución del titular del órgano administrativo competente por razón de la materia o del órgano ejecutivo competente del organismo o entidad de derecho público, según corresponda, y se publicará en la sede electrónica o sede electrónica asociada. La resolución expresará los recursos que procedan contra la actuación, el órgano administrativo o judicial, en su caso, ante el que hubieran de presentarse y plazo para interponerlos, sin perjuicio de que las personas interesadas puedan ejercitar cualquier otro que estimen oportuno y establecerá medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos de las personas interesadas.

3. En el ámbito de las Entidades Locales, en caso de actuación administrativa automatizada se estará a lo dispuesto en la disposición adicional octava del Real Decreto 128/2018, de 16 de marzo, por el que se regula el régimen jurídico de los funcionarios de Administración Local con habilitación de carácter nacional.

Artículo 14. *Régimen de subsanación.*

1. Si existe la obligación del interesado de relacionarse a través de medios electrónicos y aquel no los hubiese utilizado, el órgano administrativo competente en el ámbito de actuación requerirá la correspondiente subsanación, advirtiendo al interesado, o en su caso su representante, que, de no ser atendido el requerimiento en el plazo de diez días, se le tendrá por desistido de su solicitud o se le podrá declarar decaído en su derecho al trámite correspondiente, previa resolución que deberá ser dictada en los términos previstos en el artículo 21 de la Ley 39/2015, de 1 de octubre.

Este régimen de subsanación será asimismo aplicable a las personas físicas no obligadas a relacionarse a través de medios electrónicos con las Administraciones Públicas que, de acuerdo con lo dispuesto en el artículo 3.2, hayan ejercitado su derecho a relacionarse electrónicamente con la Administración Pública de que se trate.

Cuando se trate de una solicitud de iniciación del interesado, la fecha de la subsanación se considerará a estos efectos como fecha de presentación de la solicitud de acuerdo con el artículo 68.4 de dicha ley.

2. De acuerdo con lo establecido en el artículo 39.1 de este Reglamento, en el caso de que las Administraciones Públicas hayan determinado los formatos y estándares a los que deberán ajustarse los documentos presentados por el interesado, si este incumple dicho requisito se le requerirá para que, en el plazo de diez días, subsane el defecto advertido en los términos establecidos en los artículos 68.1, cuando se trate de una solicitud de iniciación, y 73.2, cuando se trate de otro acto, ambos de la Ley 39/2015, de 1 de octubre, con la indicación de que, si así no lo hiciera y previa resolución que deberá ser dictada en los términos previstos en el artículo 21 de dicha ley, se le tendrá por desistido de su solicitud o se le podrá declarar decaído en su derecho al trámite correspondiente, respectivamente.

3. En el caso de que el escrito o solicitud presentada adolezca de cualquier otro defecto subsanable, por la falta de cumplimiento de los requisitos exigidos en los artículos 66, 67 y 73 de la Ley 39/2015, de 1 de octubre, o por la falta de otros requisitos exigidos por la legislación específica aplicable, se requerirá su subsanación en el plazo de diez días, en los términos de los artículos 68.1 y 73.1 de la citada ley. Este plazo podrá ser ampliado hasta cinco días, a petición del interesado o a iniciativa del órgano, cuando la aportación de los documentos requeridos, en su caso, presente dificultades especiales, siempre que no se trate de procedimientos selectivos o de concurrencia competitiva.

CAPÍTULO II

De la identificación y autenticación de las Administraciones Públicas y las personas interesadas

Sección 1.ª Disposiciones comunes a la identificación y autenticación y condiciones de interoperabilidad

Artículo 15. *Sistemas de identificación, firma y verificación.*

1. Las Administraciones Públicas admitirán, en sus relaciones por medios electrónicos, sistemas de firma electrónica que sean conformes a lo establecido en la normativa vigente sobre firma electrónica y resulten adecuados para garantizar la identificación de las personas interesadas y, en su caso, la autenticidad e integridad de los documentos electrónicos.

2. Las Administraciones Públicas podrán utilizar los siguientes sistemas para su identificación electrónica y para garantizar el origen e integridad de los documentos electrónicos:

a) Sistemas de identificación de las sedes electrónicas y sedes electrónicas asociadas.

b) Sello electrónico basado en un certificado electrónico cualificado y que reúna los requisitos exigidos por la legislación de firma electrónica.

c) Sistemas de firma electrónica para la actuación administrativa automatizada.

d) Firma electrónica del personal al servicio de las Administraciones Públicas.

e) Intercambio electrónico de datos en entornos cerrados de comunicación, conforme a lo específicamente acordado entre las partes.

3. Las personas interesadas podrán utilizar los siguientes sistemas de identificación y firma en sus relaciones electrónicas con las Administraciones Públicas:

a) De acuerdo con lo previsto en el artículo 9.2 de la Ley 39/2015, de 1 de octubre, los interesados podrán identificarse electrónicamente ante las Administraciones Públicas a través de los sistemas descritos en las letras a), b) y c) de dicho artículo. En este último supuesto los sistemas deberán ser autorizados previamente por la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital, que solo podrá ser denegada por motivos de seguridad pública, previo informe vinculante de la Secretaría de Estado de Seguridad del Ministerio del Interior.

b) Asimismo, se considerarán válidos a efectos de firma electrónica ante las Administraciones Públicas los sistemas previstos en las letras a), b) y c) del artículo 10.2 de la Ley 39/2015, de 1 de octubre.

c) De acuerdo con lo previsto en el artículo 10.4 de la Ley 39/2015, de 1 de octubre, cuando así lo disponga expresamente la normativa reguladora aplicable, las Administraciones Públicas podrán admitir los sistemas de identificación previstos en dicha ley como sistema de firma cuando permitan acreditar la autenticidad de la expresión de la voluntad y consentimiento de los interesados.

4. La Administración no será responsable de la utilización por terceras personas de los medios de identificación personal y firma electrónica del interesado, salvo que concurran los requisitos establecidos en el artículo 32 de la Ley 40/2015, de 1 de octubre, para la exigencia de responsabilidad patrimonial.

Artículo 16. *Plataformas de verificación de certificados electrónicos y de otros sistemas de identificación.*

1. La Administración General del Estado dispondrá de una plataforma para la verificación de la vigencia y del contenido de los certificados cualificados admitidos en el sector público. El sistema deberá permitir que tal verificación se pueda llevar a cabo de forma libre y gratuita, para el sector público.

La Secretaría General de Administración Digital será el órgano responsable de esta plataforma, que estará disponible para todo el sector público previa formalización del correspondiente instrumento de adhesión.

2. Esta plataforma dispondrá de una declaración de prácticas de validación en la que se detallarán las obligaciones que se comprometen a cumplir tanto la plataforma como las personas usuarias de la misma en relación con los servicios de verificación. Esta declaración estará disponible al público por vía electrónica y con carácter gratuito.

3. Los prestadores cualificados de servicios de confianza deberán facilitar a esta plataforma el acceso electrónico y gratuito para la verificación de la vigencia de los certificados electrónicos emitidos por aquellos en virtud de su cualificación de acuerdo con la legislación aplicable en materia de servicios electrónicos de confianza.

Artículo 17. *Política de firma electrónica y de certificados en el ámbito estatal.*

1. La política de firma electrónica y de certificados en el ámbito estatal, está constituida por las directrices y normas técnicas aplicables a la utilización de certificados y firma electrónica.

2. Sin perjuicio de las obligaciones de los prestadores de servicios de confianza previstas en la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza y resto de normativa vigente, la política de firma electrónica y certificados deberá contener en todo caso:

a) La definición de su ámbito de aplicación.

b) Los requisitos de las firmas electrónicas presentadas ante los órganos de la Administración General del Estado y de sus organismos públicos y entidades de derecho público vinculados o dependientes.

c) Las especificaciones técnicas y operativas para la definición y prestación de los servicios de confianza asociados a las nuevas formas de identificación y autenticación de la Administración General del Estado y de sus organismos públicos y entidades vinculados o dependientes recogidas en este Reglamento.

3. La política de firma electrónica y certificados en el ámbito estatal será aprobada por Resolución de la persona titular de la Secretaría de Estado de Digitalización e Inteligencia Artificial y se publicará en el «Boletín Oficial del Estado» y en la sede electrónica del PAGe de la Administración General del Estado.

Sección 2.ª Identificación electrónica de las administraciones públicas y autenticación del ejercicio de su competencia

Artículo 18. *Identificación de las sedes electrónicas y de las sedes electrónicas asociadas.*

1. De acuerdo con lo previsto en el artículo 38 de la Ley 40/2015, de 1 de octubre, las sedes electrónicas y sedes electrónicas asociadas utilizarán, para identificarse y garantizar

una comunicación segura con las mismas, certificados cualificados de autenticación de sitio web o medio equivalente. Dichos certificados electrónicos se ajustarán a lo señalado en el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad, y la normativa vigente en materia de identidad y firma electrónica.

2. En el ámbito estatal las sedes electrónicas y sedes electrónicas asociadas se identificarán mediante certificados cualificados de autenticación de sitio web.

Con carácter adicional y para su identificación inmediata, los ciudadanos y ciudadanas dispondrán de la información general obligatoria que debe constar en las mismas de acuerdo con lo establecido en este Reglamento. Las direcciones electrónicas que tengan la condición de sede electrónica o sede electrónica asociada deberán hacerlo constar de forma visible e inequívoca. Para facilitar su identificación, seguirán las disposiciones generales que se establezcan para la imagen institucional de la Administración General del Estado y su dirección electrónica incluirá el nombre de dominio «.gob.es».

Artículo 19. *Identificación mediante sello electrónico basado en certificado electrónico cualificado que reúna los requisitos exigidos por la legislación de firma electrónica.*

1. De acuerdo con lo previsto en el artículo 40 de la Ley 40/2015, de 1 de octubre, las Administraciones Públicas podrán identificarse mediante el uso de un sello electrónico basado en un certificado electrónico cualificado que reúna los requisitos exigidos por la legislación de firma electrónica. Estos certificados electrónicos incluirán el número de identificación fiscal y la denominación correspondiente, así como, en su caso, la identidad de la persona titular en el caso de los sellos electrónicos de órganos administrativos.

2. La relación de sellos electrónicos utilizados por cada Administración Pública, incluyendo las características de los certificados electrónicos y los prestadores que los expiden, deberá ser pública y accesible por medios electrónicos, publicándose en la sede electrónica o sede asociada o en el portal de internet correspondiente. Además, cada Administración Pública adoptará las medidas adecuadas para facilitar la verificación de sus sellos electrónicos.

3. En el ámbito estatal, la creación de sellos electrónicos se realizará mediante resolución de la persona titular de la Subsecretaría del Ministerio o de la persona titular de la Presidencia o de la Dirección del organismo público o entidad de derecho público vinculado o dependiente, que se publicará en la sede electrónica o sede electrónica asociada correspondiente. En dicha resolución deberá constar:

a) El órgano, organismo público o entidad de derecho público vinculado o dependiente titular del sello, que será el responsable de su utilización, con indicación de su Ministerio de adscripción, vinculación o dependencia.

b) Características técnicas generales del sistema de firma y certificado aplicable.

c) Servicio de validación para la verificación del certificado.

d) Actuaciones y procedimientos en los que podrá ser utilizado.

4. Los certificados de sello electrónico en el ámbito estatal tendrán, al menos, los siguientes contenidos:

a) Descripción del tipo de certificado, con la denominación «sello electrónico».

b) Nombre del suscriptor.

c) Número de identificación fiscal del suscriptor.

Artículo 20. *Sistemas de firma electrónica para la actuación administrativa automatizada.*

1. De acuerdo con lo previsto en el artículo 42 de la Ley 40/2015, de 1 de octubre, en la tramitación administrativa automatizada de los procedimientos, cada Administración Pública podrá determinar los supuestos de utilización de los siguientes sistemas de firma electrónica:

a) Sello electrónico de Administración Pública, órgano, organismo público o entidad de derecho público, a que se refiere el artículo 19 de este Reglamento, basado en certificado electrónico cualificado que reúna los requisitos exigidos por la legislación de firma electrónica.

b) Código seguro de verificación vinculado a la Administración Pública, órgano, organismo público o entidad de derecho público, en los términos y condiciones establecidos,

permitiéndose en todo caso la comprobación de la integridad del documento mediante el acceso a la sede electrónica correspondiente.

2. Cada Administración determinará los medios admitidos para la firma electrónica en las entidades de derecho privado vinculadas o dependientes cuando estas tramiten procedimientos de forma automatizada en el ejercicio de potestades administrativas.

Artículo 21. *Sistemas de firma basados en código seguro de verificación para la actuación administrativa automatizada.*

1. De acuerdo con lo previsto en el artículo 42.b) de la Ley 40/2015, de 1 de octubre, las Administraciones Públicas podrán utilizar sistemas de código seguro de verificación de documentos en el desarrollo de actuaciones automatizadas.

Dicho código vinculará al órgano, organismo público o entidad de derecho público y, en su caso, a la persona firmante del documento, permitiéndose en todo caso la comprobación de la integridad del documento en la sede electrónica o sede electrónica asociada correspondiente mediante un procedimiento de verificación directo y gratuito para las personas interesadas.

2. El sistema de código seguro de verificación deberá garantizar, en todo caso:

a) El origen e integridad de los documentos mediante el acceso a la sede electrónica o sede electrónica asociada correspondiente.

b) El carácter único del código generado para cada documento.

c) Su vinculación con el documento generado y, en su caso, con el firmante. El código seguro de verificación y la dirección electrónica de acceso a la sede electrónica o sede electrónica asociada deberán integrarse preferentemente en todas las páginas del documento firmado con dicho código. Cualquier modificación del documento generado dará lugar a un nuevo documento con un código seguro de verificación diferente.

d) La posibilidad de verificar el documento en la sede electrónica o sede electrónica asociada, como mínimo, por el tiempo que se establezca en la resolución que autorice la utilización de este procedimiento. Una vez que el documento deje de estar disponible en la sede electrónica o sede electrónica asociada, su disponibilidad por otros cauces se regirá por lo dispuesto en la estrategia de conservación implantada por cada Administración Pública a través de su política de gestión documental.

e) Un acceso restringido al documento a quien disponga del código seguro de verificación, sin perjuicio de las garantías adicionales que se puedan establecer.

3. En las comunicaciones de documentos electrónicos a otros órganos, organismos o entidades y cuando así lo determinen las partes implicadas, la interoperabilidad se garantizará mediante la superposición al código seguro de verificación de un sello electrónico de los previstos en el artículo 42 de la Ley 40/2015, de 1 de octubre, como mecanismo de verificación automática del origen e integridad de los documentos electrónicos en los términos que establezca la Norma Técnica de Interoperabilidad de Documento Electrónico.

4. En el ámbito estatal, la utilización de este sistema requerirá resolución de la persona titular de la Subsecretaría del Ministerio o de la persona titular de la Presidencia o de la Dirección del organismo público o entidad de derecho público vinculado o dependiente, previo informe del Centro Criptológico Nacional y de la Secretaría General de Administración Digital.

La orden o resolución de creación deberá incluir:

a) Actuaciones a las que es de aplicación el sistema.

b) Órganos responsables de la aplicación del sistema.

c) Disposiciones que resultan de aplicación a la actuación.

d) Sede electrónica o sede electrónica asociada a la que pueden acceder las personas interesadas para la verificación del contenido de la actuación o documento.

e) Plazo de disponibilidad para la verificación en la sede electrónica o sede electrónica asociada del código seguro de verificación aplicado a un documento. Este plazo será al menos de cinco años, salvo que en la normativa especial por razón de la materia se prevea un plazo superior. Transcurrido este tiempo, será necesario solicitarlo al órgano de la

Administración Pública, organismo público o entidad de derecho público que emitió el documento. En este caso, cuando utilice medios electrónicos, la certificación de la verificación se realizará mediante firma electrónica del titular del órgano competente o del empleado o empleada público que tenga atribuida la actuación por aquel órgano.

Artículo 22. *Sistemas de firma electrónica del personal al servicio de las Administraciones Públicas.*

1. De acuerdo con lo previsto en el artículo 43 de la Ley 40/2015, de 1 de octubre, sin perjuicio de lo previsto en los artículos 18, 19 y 20 de este Reglamento, la actuación de una Administración Pública, organismo público o entidad de derecho público, cuando utilice medios electrónicos, se realizará mediante firma electrónica del titular del órgano competente o del empleado o empleada público a través del que se ejerza la competencia.

2. Cada Administración Pública determinará los sistemas de firma electrónica que debe utilizar su personal. Estos sistemas podrán identificar de forma conjunta al titular del puesto de trabajo o cargo y a la Administración u órgano en la que presta sus servicios.

3. Los certificados electrónicos de empleado público serán cualificados y se ajustarán a lo señalado en el Esquema Nacional de Interoperabilidad y la legislación vigente en materia de identidad y firma electrónica.

4. Cada Administración determinará los medios admitidos para la firma electrónica en las entidades de derecho privado vinculadas o dependientes de esta cuando tramiten procedimientos en el ejercicio de potestades administrativas.

Artículo 23. *Certificados electrónicos de empleado público con número de identificación profesional.*

1. Sin perjuicio de lo previsto en el artículo 22.3 de este Reglamento, de acuerdo con lo previsto en el artículo 43.2 de la Ley 40/2015, de 1 de octubre, los prestadores cualificados de servicios de confianza podrán consignar un número de identificación profesional en el certificado electrónico de empleado público, a petición de la Administración en la que presta servicios el empleado o empleada de que se trate, si dicho certificado se va a utilizar en actuaciones que afecten a información clasificada, a la seguridad pública, a la defensa nacional o a otras actuaciones para cuya realización esté legalmente justificado el anonimato. Estos certificados se denominarán «certificados electrónicos de empleado público con número de identificación profesional».

2. En el ámbito estatal corresponderá solicitar la consignación de un número de identificación profesional del empleado o empleada público a la persona titular de la Subsecretaría del ministerio o a la persona titular de la Presidencia o de la Dirección del organismo público o entidad de derecho público en el que preste servicios el empleado o empleada público.

3. La Administración solicitante del certificado conservará la documentación acreditativa de la identidad del titular.

4. Los certificados electrónicos de empleado público con número de identificación profesional serán cualificados y se ajustarán a lo previsto en el Esquema Nacional de Interoperabilidad y la legislación vigente en materia de identidad y firma electrónica y tendrán idéntico uso, capacidad y funcionalidad que el certificado electrónico de empleado público, aunque limitados a las actuaciones que justificaron su emisión.

5. Las autoridades públicas competentes y los órganos judiciales, en el ejercicio de sus funciones y de acuerdo con la normativa vigente, podrán solicitar la revelación de la identidad del titular de un certificado de empleado público con número de identificación profesional mediante petición oficial dirigida a la Administración responsable de su custodia.

Artículo 24. *Sistemas de identificación y firma electrónica del personal al servicio de la Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes.*

1. El personal al servicio de la Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes, podrá identificarse con aquellos sistemas que, entre los previstos en la Ley 39/2015, de 1 de octubre, se

establezcan en función del nivel de seguridad que corresponda al trámite de que se trate de acuerdo al Esquema Nacional de Seguridad.

2. Dicho personal podrá firmar mediante sistemas de firma electrónica basados en certificados electrónicos cualificados facilitados específicamente a sus empleados y empleadas. Estos sistemas podrán ser utilizados por estos en el desempeño efectivo de su puesto de trabajo, para los trámites y actuaciones que realicen por razón del mismo, o para relacionarse con las Administraciones públicas cuando estas lo admitan.

3. Se podrá disponer de sistemas de identificación de personal basados en repositorios de empleados públicos que permitan la relación de los empleados y empleadas públicos con servicios y aplicaciones necesarios para el ejercicio de sus funciones que en todo caso garanticen lo previsto en el Esquema Nacional de Seguridad.

4. Los registros de personal de la Administración General del Estado podrán recoger los datos para la identificación electrónica de los empleados y empleadas públicos, así como su cesión a sistemas de identificación de personal basados en repositorios de identidades de empleados públicos.

Artículo 25. *Intercambio electrónico de datos en entornos cerrados de comunicación.*

1. De acuerdo con lo previsto en el artículo 44 de la Ley 40/2015, de 1 de octubre, los documentos electrónicos transmitidos en entornos cerrados de comunicaciones establecidos entre Administraciones Públicas, órganos, organismos públicos y entidades de derecho público, serán considerados válidos a efectos de autenticación e identificación de los emisores y receptores en las condiciones establecidas en este artículo.

2. Cuando los participantes en las comunicaciones pertenezcan a una misma Administración Pública, esta establecerá las condiciones y garantías por las que se regirá, que comprenderán, al menos, la relación de emisores y receptores autorizados y la naturaleza de los datos a intercambiar.

3. Cuando los participantes pertenezcan a distintas Administraciones Públicas, las condiciones y garantías citadas en el apartado anterior se establecerán mediante convenio suscrito entre aquellas.

4. En el ámbito estatal, las condiciones y garantías a que se refiere el apartado 2 serán establecidas por la Secretaría General de Administración Digital.

5. En todo caso deberá garantizarse la seguridad del entorno cerrado de comunicaciones y la protección de los datos que se transmitan conforme a los requisitos establecidos en el Esquema Nacional de Seguridad

Sección 3.ª Identificación y firma de las personas interesadas

Artículo 26. *Sistemas de identificación de las personas interesadas en el procedimiento.*

1. De acuerdo con lo previsto en la Ley 39/2015, de 1 de octubre, los interesados podrán identificarse electrónicamente ante las Administraciones Públicas a través de cualquier sistema que cuente con un registro previo como usuario que permita garantizar su identidad.

2. En particular, de acuerdo con lo previsto en el artículo 9.2 de la Ley 39/2015, de 1 de octubre, serán admitidos los siguientes sistemas de identificación electrónica:

a) Sistemas basados en certificados electrónicos cualificados de firma electrónica expedidos por prestadores incluidos en la «Lista de confianza de prestadores cualificados de servicios de confianza».

b) Sistemas basados en certificados electrónicos cualificados de sello electrónico expedidos por prestadores incluidos en la «Lista de confianza de prestadores cualificados de servicios de confianza».

c) Sistemas de clave concertada y cualquier otro sistema que las Administraciones Públicas consideren válido, en los términos y condiciones que se establezca, siempre que cuenten con un registro previo como usuario que permita garantizar su identidad, previa autorización por parte de la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital, que solo podrá ser denegada por motivos de seguridad pública, previo informe vinculante de la Secretaría de Estado de Seguridad del Ministerio del Interior.

Las Administraciones Públicas deberán garantizar que la utilización de uno de los sistemas previstos en las letras a) y b) sea posible para todo procedimiento, aun cuando se admita para ese mismo procedimiento alguno de los previstos en la letra c).

Artículo 27. *Atributos mínimos de los certificados electrónicos cuando se utilizan para la identificación de las personas interesadas ante las Administraciones Públicas.*

1. Los sistemas basados en certificados cualificados de firma electrónica admitidos por las Administraciones Públicas para la identificación electrónica de persona física a que se refiere el artículo 9.2.a) de la Ley 39/2015, de 1 de octubre, emitidos al amparo de la Ley 6/2020, de 11 de noviembre, deberán contener como atributos, al menos, su nombre y apellidos y su número de Documento Nacional de Identidad, Número de Identificación de Extranjero, Número de Identificación Consular Central o Número de Identificación Fiscal que conste como tal de manera inequívoca. La comprobación de la identidad y otras circunstancias de los solicitantes del certificado se realizará de conformidad con lo previsto en el artículo 7 de la Ley 6/2020, de 11 de noviembre.

2. Los certificados electrónicos cualificados de representante de persona jurídica deberán contener, como mínimo, la denominación y el Número de Identificación Fiscal de la persona jurídica y el nombre y apellidos y número de Documento Nacional de Identidad, o Número de Identificación de Extranjero o Número de Identificación Fiscal de la persona que actúa como representante.

3. Los sistemas basados en certificados cualificados de sello electrónico admitidos por las Administraciones Públicas para la identificación electrónica de persona jurídica a que se refiere el artículo 9.2.b) de la Ley 39/2015, de 1 de octubre, emitidos al amparo de la Ley 6/2020, de 11 de noviembre, deberán contener, como mínimo, su denominación y su Número de Identificación Fiscal.

Artículo 28. *Sistemas de clave concertada y otros sistemas de identificación de las personas interesadas.*

1. Los sistemas de clave concertada o cualquier otro sistema que las Administraciones Públicas consideren válidos, admitidos para la identificación electrónica de persona física de conformidad con el artículo 9.2.c) de la Ley 39/2015, de 1 de octubre, deberán ajustarse a lo previsto en el Esquema Nacional de Seguridad y contener, como mínimo, el nombre y apellidos y el número de Documento Nacional de Identidad, Número de Identificación de Extranjero, Número de Identificación Consular Central o Número de Identificación Fiscal y, para los casos en que así se establezca en la definición del sistema, el número de pasaporte.

2. Los sistemas de identificación a que se refiere el apartado anterior deberán ser autorizados previamente por la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital, que solo podrá ser denegada por motivos de seguridad pública, previo informe vinculante de la Secretaría de Estado de Seguridad del Ministerio del Interior.

3. En el ámbito estatal, la creación de los nuevos sistemas de identificación será aprobada por orden de la persona titular del Ministerio o, en su caso, resolución de la persona titular de la Presidencia o de la Dirección del organismo público o entidad de derecho público vinculado o dependiente por razón del ámbito material en que se vaya a utilizar, previa autorización de la Secretaría General de Administración Digital a que se refiere el apartado anterior.

Cuando el nuevo sistema se refiera a la totalidad de la Administración General del Estado se requerirá Acuerdo del Consejo de Ministros a propuesta de la persona titular del Ministerio de Asuntos Económicos y Transformación Digital. En este caso, este sistema deberá estar accesible a través de la Plataforma común del Sector Público Administrativo Estatal para la identificación, autenticación y firma electrónica mediante el uso de claves concertadas.

Artículo 29. *Sistemas de firma electrónica de las personas interesadas admitidos por las Administraciones Públicas y régimen de uso.*

1. De acuerdo con lo previsto en el artículo 10.2 de la Ley 39/2015, de 1 de octubre, en el caso de que los interesados optaran por relacionarse con las Administraciones Públicas a través de medios electrónicos, se considerarán válidos a efectos de firma:

a) Sistemas de firma electrónica reconocida o cualificada y avanzada basados en certificados electrónicos cualificados de firma electrónica expedidos por prestadores incluidos en la «Lista de confianza de prestadores cualificados de servicios de confianza».

b) Sistemas de sello electrónico cualificado y de sello electrónico avanzado basados en certificados electrónicos cualificados de sello electrónico incluidos en la «Lista de confianza de prestadores cualificados de servicios de confianza».

c) Cualquier otro sistema que las Administraciones Públicas consideren válido, en los términos y condiciones que se establezca, siempre que cuente con un registro previo como usuario que permita garantizar su identidad.

Las Administraciones Públicas deberán garantizar que la utilización de uno de los sistemas previstos en las letras a) y b) sea posible para todos los procedimientos en todos sus trámites, aun cuando adicionalmente se permita alguno de los previstos al amparo de lo dispuesto en la letra c).

2. El uso de la firma electrónica no excluye la obligación de incluir en el documento o comunicación electrónica los datos de identificación del interesado y, en su caso, del representante o la representante, que sean necesarios de acuerdo con la legislación que le sea aplicable.

3. Los sistemas de firma electrónica que usen las personas interesadas permitirán que las Administraciones Públicas puedan verificar los datos consignados de la firma, de manera que se pueda vincular su identidad con el acto de firma.

4. Los sistemas de firma electrónica previstos en la letra c) del apartado 1 deberán contar con la previa autorización de la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital, que solo podrá ser denegada por motivos de seguridad pública, previo informe vinculante de la Secretaría de Estado de Seguridad del Ministerio del Interior. Asimismo, deberán cumplir con lo previsto en el Real Decreto 3/2010, de 8 de enero.

5. De acuerdo con lo previsto en el artículo 10.4 de la Ley 39/2015, de 1 de octubre, cuando así lo disponga expresamente la normativa reguladora aplicable, las Administraciones Públicas podrán admitir los sistemas de identificación previstos en dicha ley como sistema de firma cuando permitan acreditar la autenticidad de la expresión de la voluntad y consentimiento de las personas interesadas.

Artículo 30. *Identificación o firma electrónica de las personas interesadas mediante personal funcionario público habilitado.*

1. De acuerdo con lo previsto en el segundo párrafo del artículo 12.2 de la Ley 39/2015 de 1 de octubre, si algún interesado no incluido en los apartados 2 y 3 del artículo 14 de la ley no dispusiera de los medios electrónicos necesarios para su identificación o firma electrónica en el procedimiento administrativo, estas podrán ser válidamente realizadas por personal funcionario público habilitado mediante el uso del sistema de firma electrónica del que esté dotado para ello. En este caso, será necesario que el interesado se identifique ante el funcionario o funcionaria y preste su consentimiento expreso para esta actuación, de lo que deberá quedar constancia por escrito para los casos de discrepancia o litigio.

El funcionario habilitado entregará al interesado toda la documentación acreditativa del trámite realizado, así como una copia del documento de consentimiento expreso cumplimentado y firmado, cuyo formulario estará disponible en el Punto de Acceso General Electrónico de la respectiva Administración

2. En el ámbito estatal la identificación y firma electrónica del interesado conforme al procedimiento descrito en el apartado anterior se realizará necesariamente por un funcionario público inscrito a tal efecto en el Registro de Funcionarios Habilitados de la Administración General del Estado.

La identificación o firma electrónica en el procedimiento por personal funcionario público habilitado sólo será válida para los trámites y actuaciones que haya determinado con carácter previo cada ministerio, organismo público o entidad de derecho público vinculado o dependiente y en los términos que se especifiquen mediante orden conjunta de la persona titular del Ministerio de Política Territorial y Función Pública y de la persona titular del Ministerio de Asuntos Económicos y Transformación Digital. En el PAGe de la Administración General del Estado y en las sedes electrónicas asociadas de cada ministerio o en la sede electrónica o sede asociada del organismo público o entidad de derecho público en su ámbito de competencia, se mantendrá una relación pública, permanentemente actualizada, de dichos trámites y actuaciones.

Artículo 31. *Registro de Funcionarios Habilitados de la Administración General del Estado.*

1. Se crea el Registro de Funcionarios Habilitados en el ámbito de la Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes, en el que constarán inscritos:

a) El personal funcionario habilitado para la identificación y firma electrónica de las personas interesadas en aquellos trámites y procedimientos que se determinen por el ministerio, organismo o entidad competente para su tramitación.

b) El personal funcionario habilitado para la expedición de copias auténticas. Esta habilitación será conferida por los órganos a los que corresponda la emisión de los documentos originales, su custodia, el archivo de documentos o que en sus normas de competencia así se haya previsto.

c) El personal funcionario habilitado que presta servicio en las oficinas de asistencia en materia de registros de la Administración General del Estado, que estará habilitados para la identificación y firma electrónica de las personas interesadas en aquellos trámites y procedimientos que se determinen y para la expedición de copias auténticas electrónicas de cualquier documento que estas presenten para que se remita desde la Oficina a la unidad competente para su incorporación a un expediente administrativo.

2. El Registro de Funcionarios Habilitados será gestionado por la Secretaría de Estado de Política Territorial y Función Pública del Ministerio de Política Territorial y Función Pública, en colaboración con la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital. Este Registro será interoperable con los sistemas equivalentes que ya existan en el ámbito de la Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes.

3. Este Registro deberá ser plenamente interoperable con los registros u otros sistemas equivalentes que se creen por las comunidades autónomas y las entidades locales a los efectos de comprobar la validez de las citadas habilitaciones.

4. Mediante orden conjunta de la persona titular del Ministerio de Política Territorial y Función Pública y de la persona titular del Ministerio de Asuntos Económicos y Transformación Digital se regulará el funcionamiento del Registro de Funcionarios Habilitados

Sección 4.ª Acreditación de la representación de las personas interesadas

Artículo 32. *Acreditación en la actuación por medio de representante.*

1. De acuerdo con lo previsto en el artículo 5 de la Ley 39/2015, de 1 de octubre, las personas interesadas con capacidad de obrar podrán actuar ante las Administraciones Públicas por medio de representante, bien sea una persona física con capacidad de obrar bien sea una persona jurídica cuando así esté previsto en sus Estatutos.

2. Los representantes de las personas interesadas obligadas a relacionarse electrónicamente con las Administraciones Públicas están obligados a relacionarse electrónicamente en el ejercicio de dicha representación, de acuerdo con el artículo 14.2 de la Ley 39/2015, de 1 de octubre.

3. La representación puede acreditarse mediante cualquier medio válido en Derecho que deje constancia fidedigna de su existencia, entre otros:

a) Mediante apoderamiento apud acta efectuado por comparecencia personal en las oficinas de asistencia en materia de registros o comparecencia electrónica en la correspondiente sede electrónica o sede electrónica asociada.

b) Mediante acreditación de su inscripción en el registro electrónico de apoderamientos de la Administración Pública competente o en sus registros particulares de apoderamientos.

c) Mediante un certificado electrónico cualificado de representante.

d) Mediante documento público cuya matriz conste en un archivo notarial o de una inscripción practicada en un registro mercantil.

4. En el caso de actuaciones en nombre de persona jurídica, la capacidad de representación podrá acreditarse también mediante certificado electrónico cualificado de representante, entendiéndose en tal caso que el poder de representación abarca cualquier actuación ante cualquier Administración Pública.

5. Asimismo, de acuerdo con lo previsto en el artículo 5.7 de la Ley 39/2015, de 1 de octubre, las Administraciones Públicas podrán habilitar con carácter general o específico a personas físicas o jurídicas autorizadas para la realización de determinadas transacciones por medios electrónicos en representación de las personas interesadas. En la sede electrónica o sede electrónica asociada de cada una de las Administraciones Públicas se publicarán los trámites electrónicos que podrán realizarse con esta representación.

Artículo 33. *Registro Electrónico de Apoderamientos de la Administración General del Estado.*

1. A los efectos previstos en el artículo anterior y de acuerdo con el artículo 6 de la Ley 39/2015, de 1 de octubre, en el Registro Electrónico de Apoderamientos de la Administración General del Estado se inscribirán los apoderamientos de carácter general previstos en el artículo 6.4.a) de dicha ley otorgados «apud acta» a favor de representante, presencial o electrónicamente, por quien ostente la condición de interesado en un procedimiento administrativo para actuar en su nombre ante las Administraciones Públicas.

Asimismo, podrán inscribirse los poderes previstos en el artículo 6.4.b) de la ley para actuar ante la Administración General del Estado o ante un organismo público o entidad de Derecho Público vinculado o dependiente de la misma que no cuente con un registro electrónico de apoderamientos particular. Por último, podrán inscribirse los poderes previstos en el artículo 6.4.c) de la ley otorgados para realizar determinados trámites y actuaciones especificados en el poder ante los órganos de la Administración General del Estado o ante un organismo público o entidad de derecho público vinculado o dependiente de dicha Administración que no cuente con el citado registro particular.

Constará en el Registro el bastanteo del poder realizado por los servicios jurídicos correspondientes, sin perjuicio de la apreciación concreta de su suficiencia en la actuación, trámite o procedimiento en que se emplee.

2. El Registro Electrónico de Apoderamientos de la Administración General del Estado será gestionado por el Ministerio de Política Territorial y Función Pública con la colaboración del Ministerio de Asuntos Económicos y Transformación Digital, y será accesible desde la sede electrónica del PAGe de la Administración General del Estado así como desde las sedes y sedes electrónicas asociadas de la Administración General del Estado y de los organismos públicos o entidades de derecho público vinculados o dependientes.

3. Sin perjuicio de este registro general de apoderamientos, cada organismo público o entidad de derecho público vinculado o dependiente de la Administración General del Estado podrá disponer de un registro particular de apoderamientos en el que se inscriban los poderes otorgados por quien ostente la condición de interesado para realizar los trámites específicos de su competencia y cuya gestión corresponderá al propio organismo o entidad.

En estos registros particulares no podrán inscribirse los poderes previstos en el artículo 6.4.a) de la Ley 39/2015, de 1 de octubre.

4. El Registro Electrónico de Apoderamientos y los registros particulares deberán ser interoperables y no tienen carácter público, por lo que el interesado sólo podrá acceder a la información de los apoderamientos de los que sea poderdante o apoderado.

5. Mediante orden conjunta de la persona titular del Ministerio de Política Territorial y Función Pública y de la persona titular del Ministerio de Asuntos Económicos y

Transformación Digital se regularán los requisitos y condiciones de funcionamiento del Registro Electrónico de Apoderamientos de la Administración General del Estado.

Artículo 34. *Acreditación de la representación mediante certificado electrónico cualificado de representante.*

1. La representación podrá acreditarse ante la Administración con un certificado electrónico cualificado de representante de persona jurídica que sea acorde a lo previsto en el artículo 28 y el Anexo I del al Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones, electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (en adelante, Reglamento eIDAS) y a la Política marco de Firma Electrónica y de certificados a que hace referencia el Esquema Nacional de Interoperabilidad y, además, haya sido expedido a quien tenga un poder general para llevar a cabo cualquier actuación administrativa y ante cualquier Administración.

2. La aceptación de certificados electrónicos cualificados de representante de persona jurídica de alcance no general estará sujeta al Reglamento eIDAS, a la Política Marco de Firma Electrónica y de Certificados a que hace referencia el Esquema Nacional de Interoperabilidad y además, a los requisitos que disponga cada Administración.

Artículo 35. *Acreditación y verificación de las representaciones que resulten de un documento público notarial o certificación de un Registro Mercantil.*

1. Cuando la representación alegada resulte de un documento público notarial, o de una certificación expedida por un registro mercantil, el interesado deberá aportar la certificación registral electrónica correspondiente o al menos expresar el código seguro u otro sistema de acceso y verificación del documento electrónico.

2. Las Administraciones Públicas efectuarán la verificación de la autenticidad e integridad del traslado a papel y el acceso a los metadatos necesarios para la tramitación automatizada de la certificación registral electrónica, mediante el acceso electrónico y gratuito a la dirección electrónica que el Consejo General del Notariado o el Colegio de Registradores, respectivamente, habrán de tener habilitada a tales efectos.

3. Asimismo, las Administraciones Públicas, cuando necesiten comprobar la vigencia, revocación o cese de representaciones inscritas en el Registro Mercantil, consultarán electrónicamente y de modo gratuito el Registro Mercantil.

Artículo 36. *Autorización de representantes de terceros por la Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes.*

1. La Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes, de acuerdo con lo previsto en el artículo 5.7 de la Ley 39/2015, de 1 de octubre, podrán habilitar con carácter general o específico a personas físicas o jurídicas autorizadas para la realización de determinadas transacciones electrónicas en representación de las personas interesadas.

2. La habilitación requerirá la firma previa de un convenio entre el Ministerio, organismo público o entidad de derecho público vinculado o dependiente competente y la organización o corporación de que se trate, de acuerdo de lo previsto en el capítulo VI del título Preliminar de la Ley 40/2015, de 1 de octubre. El convenio deberá especificar, al menos, los procedimientos y trámites objeto de la habilitación, y las condiciones y obligaciones aplicables tanto a la entidad firmante del convenio, como a las personas físicas o jurídicas habilitadas y determinará la presunción de validez de la representación.

A estos efectos, podrá acordarse un modelo normalizado de convenio que permita dar soporte a esta habilitación en los términos y condiciones que las partes acuerden, conforme a lo dispuesto en la Ley 40/2015, de 1 de octubre, y que incluya como anexo el modelo individualizado de adhesión al convenio que, previendo expresamente la aceptación de su contenido íntegro, deben suscribir las personas físicas o jurídicas miembros de las organizaciones o corporaciones firmantes que se adhieran al mismo.

3. De acuerdo con lo previsto en el artículo 32.5, en el ámbito de la Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes, los trámites electrónicos que podrán realizarse con esta representación se publicarán en la sede electrónica del PAGe de la Administración General del Estado y en las respectivas sedes electrónicas o sedes electrónicas asociadas.

CAPÍTULO III

Registros, comunicaciones y notificaciones electrónicas

Sección 1.ª Registros electrónicos

Artículo 37. *Registro electrónico.*

1. Las Administraciones Públicas dispondrán de registros electrónicos para la recepción y remisión de solicitudes, escritos y comunicaciones, que deberán ser plenamente interoperables de manera que se garantice su compatibilidad informática e interconexión en los términos previstos en el artículo 16 de la Ley 39/2015, de 1 de octubre y en el artículo 60 de este Reglamento.

2. Cada Administración dispondrá de un Registro Electrónico General en el que hará el asiento de todo documento que sea presentado o que se reciba en cualquier órgano administrativo, organismo público o entidad de derecho público vinculado o dependiente. Los organismos públicos y entidades de derecho público vinculados o dependientes de cada Administración podrán disponer de su propio registro electrónico plenamente interoperable e interconectado con el Registro Electrónico General de la Administración a la que estén vinculados o de la que dependan.

3. Los registros electrónicos admitirán:

a) Documentos electrónicos normalizados correspondientes a los servicios, procedimientos y trámites que se especifiquen conforme a lo dispuesto en la norma de creación del registro, cumplimentados de acuerdo con formatos preestablecidos.

b) Cualquier solicitud, escrito o comunicación distinta de los mencionados en el párrafo anterior dirigido a cualquier Administración Pública.

4. De acuerdo con el artículo 16.8 de la Ley 39/2015, de 1 de octubre, no se tendrán por presentados en el registro aquellos documentos e información cuyo régimen especial establezca otra forma de presentación. En estos supuestos, el órgano administrativo competente para la tramitación del procedimiento comunicará esta circunstancia al interesado e informará de los requisitos exigidos por la legislación específica aplicable

Artículo 38. *Registro Electrónico General de la Administración General del Estado.*

1. El Registro Electrónico General de la Administración General del Estado será gestionado por el Ministerio de Política Territorial y Función Pública en colaboración con el Ministerio de Asuntos Económicos y Transformación Digital y se configura como el conjunto agregado de:

a) Los asientos practicados a través de las aplicaciones de que dispongan las unidades que realicen anotaciones en registro.

b) Las anotaciones que se realicen en cualquier aplicación que proporcione soporte a procedimientos específicos.

c) Las anotaciones que se practiquen por medio del servicio electrónico para la presentación de solicitudes, escritos y comunicaciones que no dispongan de modelos normalizados de presentación, independientemente de las Administraciones Públicas u organismos públicos o entidades de derecho público vinculados o dependientes a las que vayan dirigidos. Dicho servicio electrónico será accesible desde la sede electrónica del PAGe de la Administración General del Estado.

2. Las anotaciones en el Registro General de la Administración General del Estado tendrán plena eficacia y validez para todas las Administraciones Públicas.

Artículo 39. *Presentación y tratamiento de documentos en registro.*

1. Las Administraciones Públicas podrán determinar los formatos y estándares a los que deberán ajustarse los documentos presentados por las personas interesadas en el registro siempre que cumplan con lo previsto en el Esquema Nacional de Interoperabilidad y normativa correspondiente.

2. En el caso de que se detecte código malicioso susceptible de afectar a la integridad o seguridad del sistema en documentos que ya hayan sido registrados, se requerirá su subsanación al interesado que los haya aportado de acuerdo con lo previsto en el artículo 14.3 de este Reglamento.

3. Los documentos en soporte no electrónico se presentarán a través de las oficinas de asistencia en materia de registros. Cuando se presenten documentos originales o copias auténticas en soporte no electrónico, desde el momento en que sean digitalizados conforme a lo dispuesto en las correspondientes normas técnicas de interoperabilidad, tendrán la consideración de copia electrónica auténtica de documento en soporte papel con la misma validez para su tramitación que los documentos aportados en soporte papel, conforme a las previsiones del artículo 27 de la Ley 39/2015, de 1 de octubre.

4. Cuando el tamaño de los documentos registrados exceda la capacidad que se determine para el Sistema de Interconexión de Registros (SIR), su remisión a la Administración y órgano al que van dirigidos podrá sustituirse por la puesta a disposición de los documentos, previamente depositados en un repositorio de intercambio de ficheros.

En ámbito de la Administración General del Estado dicho repositorio de intercambio de ficheros será de titularidad pública y tanto los documentos depositados como los datos que estos contengan no podrán ser utilizados para fines distintos a los previstos en la normativa que regule el procedimiento para el que han sido objeto de registro.

5. Los documentos presentados en las oficinas de asistencia en materia de registro serán devueltos a las personas interesadas inmediatamente tras su digitalización o, en caso contrario, se les aplicará lo previsto en el artículo 53 de este Reglamento.

6. El archivo de los documentos intercambiados por registro corresponderá al órgano competente para la tramitación del procedimiento, de acuerdo al plazo que determine su normativa.

Artículo 40. *Oficinas de asistencia en materia de registros en el ámbito de la Administración General del Estado.*

1. Las Oficinas de asistencia en materia de registros tienen naturaleza de órgano administrativo de acuerdo con lo dispuesto en el artículo 5 de la Ley 40/2015, de 1 de octubre.

La creación de nuevas Oficinas, así como la modificación o supresión de las existentes se realizará conforme a lo previsto en el artículo 59.2 de la Ley 40/2015, de 1 de octubre.

2. La Administración General del Estado contará con un directorio geográfico de las Oficinas de asistencia en materia de registros que será gestionado por el Ministerio de Política Territorial y Función Pública. A tal efecto, el órgano del que dependa la correspondiente Oficina de asistencia deberá comunicar de forma inmediata al citado Ministerio la aprobación de la norma por la que se cree, modifique o suprima dicha oficina, de acuerdo con lo establecido en el Esquema Nacional de Interoperabilidad, garantizando su actualización permanente.

3. Las Oficinas de asistencia en materia de registros desarrollarán las siguientes funciones:

a) La digitalización de las solicitudes, escritos y comunicaciones en papel que se presenten o sean recibidos en la Oficina y se dirijan a cualquier órgano, organismo público o entidad de derecho público de cualquier Administración Pública, así como su anotación en el Registro Electrónico General o Registro electrónico de cada organismo o entidad según corresponda.

b) La anotación, en su caso, de los asientos de salida que se realicen de acuerdo con lo dispuesto en el artículo 16 de la Ley 39/2015, de 1 de octubre.

c) La emisión del correspondiente recibo que acredite la fecha y hora de presentación de solicitudes, comunicaciones y documentos que presenten las personas interesadas.

d) La expedición de copias electrónicas auténticas tras la digitalización de cualquier documento original o copia auténtica que presenten las personas interesadas y que se vaya a incorporar a un expediente administrativo a través de dicha oficina en el registro electrónico correspondiente.

e) La información en materia de identificación y firma electrónica, para la presentación de solicitudes, escritos y comunicaciones a través de medios electrónicos en los trámites y procedimientos para los que se haya conferido habilitación.

f) La identificación o firma electrónica del interesado, cuando se trate de una persona no obligada a la relación electrónica con la Administración, en los procedimientos administrativos para los que se haya previsto habilitación.

g) La práctica de notificaciones, en el ámbito de actuación de esa Oficina, cuando el interesado o su representante comparezcan de forma espontánea en la Oficina y solicite la comunicación o notificación personal en ese momento.

h) La comunicación a las personas interesadas del código de identificación del órgano, organismo público o entidad a la que se dirige la solicitud, escrito o comunicación.

i) La iniciación de la tramitación del apoderamiento presencial apud acta en los términos previstos en el artículo 6 de la Ley 39/2015, de 1 de octubre.

j) Cualesquiera otras funciones que se les atribuyan legal o reglamentariamente.

Sección 2.ª Comunicaciones y notificaciones electrónicas

Artículo 41. *Comunicaciones administrativas a las personas interesadas por medios electrónicos.*

Cuando de acuerdo con lo previsto en el artículo 14 de la Ley 39/2015, de 1 de octubre, la relación de las personas interesadas con las Administraciones Públicas deba realizarse por medios electrónicos, serán objeto de comunicación al interesado por medios electrónicos, al menos:

a) La fecha y, en su caso, hora efectiva de inicio del cómputo de plazos que haya de cumplir la Administración tras la presentación del documento o documentos en el registro electrónico, de acuerdo con lo previsto en el artículo 31.2.c) de la Ley 39/2015, de 1 de octubre.

b) La fecha en que la solicitud ha sido recibida en el órgano competente, el plazo máximo para resolver el procedimiento y para la práctica de la notificación de los actos que le pongan término, así como de los efectos del silencio administrativo, de acuerdo con lo previsto en el artículo 21.4 de la Ley 39/2015, de 1 de octubre.

c) La solicitud de pronunciamiento previo y preceptivo a un órgano de la Unión Europea y la notificación del pronunciamiento de ese órgano de la Unión Europea a la Administración instructora de acuerdo con lo previsto en el artículo 22.1.b) de la Ley 39/2015, de 1 de octubre.

d) La existencia, desde que se tenga constancia de la misma, de un procedimiento no finalizado en el ámbito de la Unión Europea que condicione directamente el contenido de la resolución, así como la finalización de dicho procedimiento de acuerdo con lo previsto en el artículo 22.1.c) de la Ley 39/2015, de 1 de octubre.

e) La solicitud de un informe preceptivo a un órgano de la misma o distinta Administración y la recepción, en su caso, de dicho informe, de acuerdo con lo previsto en el artículo 22.1.d) de la Ley 39/2015, de 1 de octubre.

f) La solicitud de previo pronunciamiento de un órgano jurisdiccional, cuando este sea indispensable para la resolución del procedimiento, así como el contenido del pronunciamiento cuando la Administración actuante tenga la constancia del mismo de acuerdo con lo previsto en el artículo 22.1.g) de la Ley 39/2015, de 1 de octubre.

g) La realización del requerimiento de anulación o revisión de actos entre administraciones previsto en el artículo 22.2.a) de la Ley 39/2015, de 1 de octubre, así como su cumplimiento o, en su caso, la resolución del correspondiente recurso contencioso-administrativo.

Artículo 42. *Práctica de las notificaciones a través de medios electrónicos.*

1. De acuerdo con lo previsto en el artículo 43.1 de la Ley 39/2015, de 1 de octubre, las notificaciones por medios electrónicos se practicarán mediante comparecencia en la sede electrónica o sede electrónica asociada de la Administración, organismo público o entidad de derecho público vinculado o dependiente actuante, a través de la Dirección Electrónica Habilitada única o mediante ambos sistemas, según disponga cada Administración, organismo público o entidad de derecho público vinculado o dependiente, debiendo quedar constancia de la fecha y hora del acceso al contenido de la misma, o del rechazo de la notificación.

En caso de que la Administración, organismo o entidad actuante lleve a cabo la puesta a disposición de las notificaciones por ambos sistemas, para el cómputo de plazos y el resto de efectos jurídicos se tomará la fecha y hora de acceso al contenido o el rechazo de la notificación por el interesado o su representante en el sistema en el que haya ocurrido en primer lugar. A tal efecto se habrá de disponer de los medios electrónicos necesarios para sincronizar de forma automatizada en uno y otro sistema la información sobre el estado de la notificación con objeto de garantizar la eficacia y seguridad jurídica en la tramitación del procedimiento.

2. Con independencia de que un interesado no esté obligado a relacionarse electrónicamente con las Administraciones Públicas o de que no haya comunicado que se le practiquen notificaciones por medios electrónicos, su comparecencia voluntaria o la de su representante en la sede electrónica o sede asociada de una Administración, organismo público o entidad de derecho público vinculado o dependiente o a través de la Dirección Electrónica Habilitada única, y el posterior acceso al contenido de la notificación o el rechazo expreso de esta tendrá plenos efectos jurídicos.

3. La notificación por comparecencia en la sede electrónica o sede electrónica asociada y a través de la Dirección Electrónica Habilitada única conlleva la puesta a disposición del interesado de un acuse de recibo que permita justificar bien el acceso al contenido de la notificación, bien el rechazo del interesado a recibirla.

El acuse contendrá, como mínimo, la identificación del acto notificado y la persona destinataria, la fecha y hora en la que se produjo la puesta a disposición y la fecha y hora del acceso a su contenido o del rechazo.

4. En los supuestos de sucesión de personas físicas o jurídicas, inter vivos o mortis causa, la persona o entidad que sucede al interesado comunicará la sucesión al órgano competente de la tramitación del procedimiento de cuya existencia tenga conocimiento. Dicha comunicación deberá efectuarse tras la efectividad de la sucesión o desde la inscripción de la defunción en el Registro Civil, en el caso de fallecimiento de persona física.

El órgano responsable de la tramitación procederá, en su caso, en procedimientos no finalizados, a autorizar a la persona o entidad sucesora el acceso a las notificaciones electrónicas ya practicadas desde la fecha del hecho causante de la sucesión y a practicar a dicha persona o entidad sucesora las notificaciones electrónicas que se produzcan en lo sucesivo. En el caso en el que la persona física sucesora no estuviera obligada a relacionarse electrónicamente con la Administración y no opte por este cauce de relación, las notificaciones que se produzcan en lo sucesivo deberán practicarse en papel, sin perjuicio de la garantía de acceso al expediente completo.

La persona o entidad que suceda al interesado en un procedimiento del que conozca su existencia debe comunicar, conforme a lo expuesto en los párrafos anteriores, la sucesión a la Administración Pública a la que corresponda la tramitación de aquel, en el plazo de 15 días hábiles, desde el día siguiente al de la efectividad de la sucesión o desde la inscripción de la defunción en el Registro Civil, en el caso de fallecimiento de persona física. Si la persona o entidad sucesora efectúa la comunicación después de dicho plazo, los defectos en la práctica de notificaciones que se deriven de este incumplimiento, que hubieran acaecido con anterioridad a dicha comunicación, le serán imputables al interesado; dándose por cumplida por la Administración, a todos los efectos, la obligación de puesta a disposición de la notificación electrónica en la sede electrónica o sede electrónica asociada, a través de la Dirección Electrónica Habilitada única o ambas, según proceda, a la persona jurídica o persona física cuya sucesión el interesado no ha hecho valer.

5. Toda notificación cuyo emisor pertenezca al ámbito estatal a que se refiere el artículo 1.2 de este Reglamento se pondrá a disposición del interesado a través de la Dirección Electrónica Habilitada única, incluyendo el supuesto previsto en el artículo 42.1 de la Ley 39/2015, de 1 de octubre. Asimismo, los emisores de ámbito estatal podrán notificar en su sede electrónica o sede electrónica asociada de forma complementaria a la puesta a disposición en la Dirección Electrónica Habilitada única.

Artículo 43. *Aviso de puesta a disposición de la notificación.*

1. De acuerdo con lo previsto en el artículo 41.6 de la Ley 39/2015, de 1 de octubre, con independencia de que la notificación se realice en papel o por medios electrónicos, las Administraciones Públicas, organismos públicos o entidades de derecho público vinculados o dependientes enviarán al interesado o, en su caso, a su representante, aviso informándole de la puesta a disposición de la notificación bien en la Dirección Electrónica Habilitada única, bien en la sede electrónica o sede electrónica asociada de la Administración, u Organismo o Entidad o, en su caso, en ambas.

La falta de práctica de este aviso, de carácter meramente informativo, no impedirá que la notificación sea considerada plenamente válida.

El aviso se remitirá al dispositivo electrónico o la dirección de correo electrónico que el interesado haya comunicado voluntariamente al efecto, o a ambos, de acuerdo con lo previsto en el artículo 41.1 de la Ley 39/2015, de 1 de octubre.

El interesado se hace responsable, por la comunicación a la Administración, organismo público o entidad de derecho público vinculado o dependiente, de que dispone de acceso al dispositivo o dirección de correo electrónico designados. En caso de que dejen de estar operativos o pierda la posibilidad de acceso, el interesado está obligado a comunicar a la Administración que no se realice el aviso en tales medios. El incumplimiento de esta obligación por parte del interesado no conllevará responsabilidad alguna para la Administración por los avisos efectuados a dichos medios no operativos.

El aviso regulado en este apartado sólo se practicará en caso de que el interesado o su representante hayan comunicado a la Administración un dispositivo electrónico o dirección de correo electrónico al efecto.

2. Cuando el interesado sea un sujeto obligado a relacionarse por medios electrónicos y la Administración emisora de la notificación no disponga de datos de contacto electrónicos para practicar el aviso de su puesta a disposición, en los procedimientos iniciados de oficio la primera notificación que efectúe la Administración, organismo o entidad se realizará en papel en la forma determinada por el artículo 42.2 de la Ley 39/2015, de 1 de octubre, advirtiendo al interesado en esa primera notificación que las sucesivas se practicarán en forma electrónica por comparecencia en la sede electrónica o sede electrónica asociada que corresponda o, en su caso, a través de la Dirección Electrónica Habilitada única según haya dispuesto para sus notificaciones la Administración, organismo o entidad respectivo, y dándole a conocer que, de acuerdo con lo previsto en el artículo 41.1 de la Ley 39/2015, de 1 de octubre, puede identificar un dispositivo electrónico, una dirección de correo electrónico o ambos para el aviso de la puesta a disposición de las notificaciones electrónicas posteriores.

3. Las Administraciones podrán crear bases de datos de contacto electrónico para la práctica de los avisos de puesta a disposición de notificaciones en su respectivo ámbito.

Artículo 44. *Notificación a través de la Dirección Electrónica Habilitada única.*

1. La Dirección Electrónica Habilitada única es el sistema de información para la notificación electrónica cuya gestión corresponde al Ministerio de Asuntos Económicos y Transformación Digital en colaboración con el Ministerio de Política Territorial y Función Pública.

2. De acuerdo con lo previsto en el artículo 7.4, la Dirección Electrónica Habilitada única se aloja en la sede electrónica del PAGe de la Administración General del Estado.

3. La adhesión a la Dirección Electrónica Habilitada única se realizará en los términos previstos en el artículo 65.

Todas las Administraciones Públicas y sus organismos públicos y entidades de derecho público vinculados o dependientes colaborarán para establecer sistemas interoperables que

permitan que las personas físicas y jurídicas puedan acceder a todas sus notificaciones a través de la Dirección Electrónica Habilitada única, tal como establece el artículo 43 de la Ley 39/2015, de 1 de octubre.

Esta previsión será aplicable con independencia de cuál sea la Administración que practica la notificación y si las notificaciones se han practicado en papel o por medios electrónicos.

4. Cuando una incidencia técnica imposibilite el funcionamiento ordinario de la Dirección Electrónica Habilitada única, una vez comunicada dicha incidencia a los órganos, organismos o entidades emisores que la utilicen como medio de notificación, estos podrán determinar una ampliación del plazo no vencido para comparecer y acceder a las notificaciones emitidas. En caso de que también pongan a disposición las notificaciones en su sede electrónica o sede electrónica asociada, deberán publicar también en esta tanto la incidencia técnica acontecida en la Dirección Electrónica Habilitada única como la ampliación concreta, en su caso, del plazo no vencido.

5. Con carácter previo al acceso al contenido de la notificación puesta a disposición del interesado en la Dirección Electrónica Habilitada única, este será informado de que de acuerdo con lo previsto en los artículos 41 y 43 de la Ley 39/2015, de 1 de octubre, dicho acceso al contenido, el rechazo expreso de la notificación o bien la presunción de rechazo por haber transcurrido el plazo de diez días naturales desde la puesta a disposición de la notificación sin acceder al contenido de la misma, dará por efectuado el trámite de notificación y se continuará el procedimiento.

6. Para dar por efectuado el trámite de notificación a efectos jurídicos, en la Dirección Electrónica Habilitada única deberá quedar constancia, con indicación de fecha y hora, del momento del acceso al contenido de la notificación, del rechazo expreso de la misma o del vencimiento del plazo previsto en el artículo 43.2 de la Ley 39/2015, de 1 de octubre.

El estado del trámite de notificación en la Dirección Electrónica Habilitada única se sincronizará automáticamente con la sede electrónica o sede electrónica asociada en la que, en su caso, la notificación también se hubiera puesto a disposición del interesado.

Artículo 45. *Notificación electrónica en sede electrónica o sede electrónica asociada.*

1. Con carácter previo al acceso al contenido de la notificación puesta a disposición del interesado en la sede electrónica o sede electrónica asociada del emisor de la misma, este será informado de que de acuerdo con lo previsto en los artículos 41 y 43 de la Ley 39/2015, de 1 de octubre, la comparecencia y acceso al contenido, el rechazo expreso de la notificación o bien la presunción de rechazo por haber transcurrido el plazo de diez días naturales desde la puesta a disposición de la notificación sin acceder al contenido de la misma dará por efectuado el trámite de notificación y se continuará el procedimiento.

2. Para dar por efectuado el trámite de notificación a efectos jurídicos, en la sede electrónica o sede electrónica asociada deberá quedar constancia, con indicación de fecha y hora, del momento del acceso al contenido de la notificación, del rechazo expreso de la misma o del vencimiento del plazo previsto en el artículo 43.2 de la Ley 39/2015, de 1 de octubre.

El estado del trámite de notificación en la sede electrónica o sede electrónica asociada se sincronizará automáticamente con la Dirección Electrónica Habilitada única si la notificación también se hubiera puesto a disposición del interesado en aquella.

3. De conformidad con el artículo 43.3 de la Ley 39/2015, de 1 de octubre, se entenderá cumplida la obligación de notificar en plazo por parte de la Administración, a que se refiere el artículo 40.4 de dicha ley, con la puesta a disposición de la notificación en la sede o en la dirección electrónica habilitada única.

TÍTULO III

Expediente administrativo electrónico

CAPÍTULO I

Documento administrativo electrónico y copias

Artículo 46. *Documento administrativo electrónico.*

1. Se entiende por documento administrativo electrónico la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico, según un formato determinado y susceptible de identificación y tratamiento diferenciado admitido en el Esquema Nacional de Interoperabilidad y normativa correspondiente, y que haya sido generada, recibida o incorporada por las Administraciones Públicas en el ejercicio de sus funciones sujetas a Derecho administrativo.

2. Cuando en el marco de un procedimiento administrativo tramitado por medios electrónicos el órgano actuante esté obligado a facilitar al interesado un ejemplar de un documento administrativo electrónico, dicho documento se podrá sustituir por la entrega de los datos necesarios para su acceso por medios electrónicos adecuados.

Artículo 47. *Requisitos de validez y eficacia de las copias auténticas de documentos.*

1. De acuerdo con lo previsto en el artículo 27.2 de la Ley 39/2015, de 1 de octubre, tendrá la consideración de copia auténtica de un documento público administrativo o privado original o de otra copia auténtica, la realizada, cualquiera que sea su soporte, por los órganos competentes de las Administraciones Públicas en las que quede garantizada la identidad del órgano que ha realizado la copia y su contenido.

2. Las copias auténticas se expedirán siempre a partir de un original o de otra copia auténtica y tendrán la misma validez y eficacia que los documentos originales.

Artículo 48. *Órganos competentes para la emisión de copias auténticas de documentos en el ámbito estatal.*

1. En el ámbito estatal, serán competentes para la expedición de copias auténticas de documentos públicos administrativos o documentos privados, que sean documentos originales o copias auténticas de documento original los siguientes órganos:

a) Los órganos a los que corresponda la emisión de los documentos originales.

b) Los órganos a los que corresponda la custodia y archivo de documentos.

c) Los órganos que hayan previsto sus normas de competencia.

d) Las oficinas de asistencia en materia de registros, respecto de los documentos originales o copias auténticas presentados por las personas interesadas para que se remitan desde la Oficina a la unidad competente para su incorporación a un expediente administrativo.

2. La expedición de copias auténticas de documentos públicos administrativos o documentos privados, que sean documentos originales o copias auténticas de documento original, podrá llevarse a cabo mediante actuación administrativa automatizada o por personal funcionario habilitado inscrito en el Registro de Funcionarios Habilitados de la Administración General del Estado al que se refiere el artículo 31 de este Reglamento.

3. Los titulares de los órganos que se relacionan en los párrafos a), b) c) y d) del apartado 1 de este artículo designarán a los funcionarios y funcionarias habilitados para la emisión de las copias electrónicas auténticas, que se llevará a cabo mediante el correspondiente proceso de digitalización.

Artículo 49. *Emisión de copias de documentos aportados en papel por el interesado.*

Cuando el interesado presente en papel una copia de un documento público administrativo o de un documento privado para incorporarlo a un expediente administrativo,

el proceso de digitalización por la Administración Pública generará una copia electrónica que tendrá el mismo valor que la copia presentada en papel.

Artículo 50. *Referencia temporal de los documentos administrativos electrónicos.*

1. Todos los documentos administrativos electrónicos deberán llevar asociadas una de las siguientes modalidades de referencia temporal, de acuerdo con lo que determinen las normas reguladoras de los respectivos procedimientos:

a) Marca de tiempo, entendiendo por tal la asignación por medios electrónicos de la fecha y, en su caso, la hora a un documento electrónico.

b) Sello electrónico cualificado de tiempo, entendiendo por tal la asignación por medios electrónicos de una fecha y hora a un documento electrónico con la intervención de un prestador cualificado de servicios de confianza que asegure la exactitud e integridad de la marca de tiempo del documento. Los sellos electrónicos de tiempo no cualificados serán asimilables a todos los efectos a las marcas de tiempo.

2. La marca de tiempo será utilizada en todos aquellos casos en los que las normas reguladoras no establezcan la utilización de un sello electrónico cualificado de tiempo

La información relativa a las marcas y sellos electrónicos cualificados de tiempo se asociará a los documentos electrónicos en la forma que determine el Esquema Nacional de Interoperabilidad y normativa correspondiente.

3. La relación de prestadores cualificados de servicios de confianza que prestan servicios de sellado de tiempo en el sector público deberá estar incluida en la «Lista de confianza de prestadores cualificados de servicios de confianza».

Artículo 51. *Configuración del expediente administrativo electrónico.*

1. El foliado de los expedientes administrativos electrónicos se llevará a cabo mediante un índice electrónico autenticado que garantizará la integridad del expediente y permitirá su recuperación siempre que sea preciso.

2. Un mismo documento electrónico podrá formar parte de distintos expedientes administrativos.

3. El índice electrónico autenticado será firmado por el titular del órgano que conforme el expediente para su tramitación o bien podrá ser sellado electrónicamente en el caso de expedientes electrónicos que se formen de manera automática, a través de un sistema que garantice su integridad.

Artículo 52. *Ejercicio del derecho de acceso al expediente electrónico y obtención de copias de los documentos electrónicos.*

De acuerdo con lo previsto en el artículo 53.1.a) de la Ley 39/2015, de 1 de octubre, el derecho de acceso de las personas interesadas que se relacionen electrónicamente con las Administraciones Públicas al expediente electrónico y, en su caso, a la obtención de copia total o parcial del mismo, se entenderá satisfecho mediante la puesta a disposición de dicho expediente en el Punto de Acceso General electrónico de la Administración competente o en la sede electrónica o sede electrónica asociada que corresponda.

A tal efecto, la Administración destinataria de la solicitud remitirá al interesado o, en su caso a su representante, la dirección electrónica o localizador que dé acceso al expediente electrónico puesto a disposición, garantizando aquella el acceso durante el tiempo que determine la correspondiente política de gestión de documentos electrónicos siempre de acuerdo con el dictamen de valoración emitido por la autoridad calificadora correspondiente, y el cumplimiento de la normativa aplicable en materia de protección de datos de carácter personal y de transparencia y acceso a la información pública y de patrimonio documental, histórico y cultural.

Artículo 53. *Tiempo de conservación y destrucción de documentos.*

1. Los documentos presentados por el interesado en soporte papel que por cualquier circunstancia no le puedan ser devueltos en el momento de su presentación, una vez digitalizados serán conservados a su disposición durante seis meses para que pueda

recogerlos, independientemente del procedimiento administrativo al que se incorporen o de la Administración Pública a que vayan dirigidos, salvo que reglamentariamente la Administración correspondiente establezca un plazo mayor.

2. Los documentos presentados por el interesado en formato electrónico dentro de un dispositivo, que por cualquier circunstancia no le puedan ser devueltos en el momento de su presentación, una vez incorporados al expediente serán conservados a su disposición durante seis meses para que pueda recogerlos, independientemente del procedimiento administrativo al que se incorporen o de la Administración Pública a que vayan dirigidos, salvo que reglamentariamente la Administración correspondiente establezca un plazo mayor.

3. Transcurrido el plazo previsto en los apartados anteriores, la destrucción de los documentos se realizará de acuerdo con las competencias del Ministerio de Cultura y Deporte o del órgano competente de la comunidad autónoma, y siempre que no se trate de documentos con valor histórico, artístico u otro relevante o de documentos en los que la firma u otras expresiones manuscritas o mecánicas confieran al documento un valor especial.

4. Cuando la generación de copias electrónicas auténticas se realice a partir de documentos originales o copias auténticas de documentos en soporte no electrónico que se conserven formando parte de sus correspondientes expedientes y series documentales en cualesquiera de las oficinas, archivos o dependencias de cualquier organismo de las Administraciones públicas, dichos documentos originales o copias auténticas de documentos en soporte no electrónico se restituirán a sus oficinas, archivos o dependencias de origen, donde les será de aplicación la normativa específica en materia de archivos y conservación del patrimonio documental en su respectivo ámbito y siguiendo lo establecido por las autoridades calificadoras que correspondan.

5. En el ámbito estatal, se estará a lo preceptuado en el Real Decreto 1164/2002, de 8 de noviembre, por el que se regula la conservación del patrimonio documental con valor histórico, el control de la eliminación de otros documentos de la Administración General del Estado y sus organismos públicos y entidades de derecho público y la conservación de documentos administrativos en soporte distinto al original.

CAPÍTULO II

Archivo electrónico de documentos

Artículo 54. *Conservación de documentos electrónicos.*

1. De acuerdo con lo previsto en el artículo 46 de la Ley 40/2015, de 1 de octubre, las Administraciones Públicas, así como sus organismos públicos y entidades de derecho público vinculados o dependientes, deberán conservar en soporte electrónico todos los documentos que formen parte de un expediente administrativo y todos aquellos documentos con valor probatorio creados al margen de un procedimiento administrativo.

La copia electrónica auténtica generada conforme a lo dispuesto en el artículo 27 de la Ley 39/2015, de 1 de octubre, tiene la consideración de patrimonio documental a efectos de aplicación de la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español o la normativa autonómica correspondiente, siendo el periodo de conservación de los documentos el establecido por las autoridades calificadoras que correspondan.

2. Cada Administración Pública, regulará los períodos mínimos de conservación de los documentos electrónicos, que formen parte del expediente de un procedimiento cuya tramitación haya concluido, conforme a su normativa específica de archivos y patrimonio documental.

Cuando se tenga conocimiento por la Administración Pública, organismo o entidad de la existencia de procedimientos judiciales que afecten o puedan afectar a documentos electrónicos, estos deberán conservarse a disposición de los órganos jurisdiccionales, hasta tanto exista constancia de la terminación del procedimiento judicial correspondiente en las sucesivas instancias, por haber recaído resolución no susceptible de recurso o procedimiento alguno ante órganos jurisdiccionales nacionales o internacionales.

3. La conservación de los documentos electrónicos deberá realizarse de forma que permita su acceso y comprenda, como mínimo, su identificación, contenido, metadatos, firma, estructura y formato.

También será posible la inclusión de su información en bases de datos siempre que, en este último caso, consten los criterios para la reconstrucción de los formularios o modelos electrónicos origen de los documentos, así como para la comprobación de la identificación o firma electrónica de dichos datos.

Los plazos de conservación de esta información están sujetos a los mismos plazos establecidos para los correspondientes documentos electrónicos.

4. Para asegurar la conservación, acceso y consulta de los documentos electrónicos archivados con independencia del tiempo transcurrido desde su emisión, se podrán trasladar los datos a otros formatos y soportes que garanticen el acceso desde diferentes aplicaciones, de acuerdo con lo previsto en el artículo 27 de la Ley 39/2015, de 1 de octubre y en la normativa específica de archivos y patrimonio documental, histórico y cultural.

Asimismo, se planificarán las actuaciones de preservación digital que garanticen la conservación a largo plazo de los documentos digitales y permitan de esta forma dar cumplimiento a lo establecido en el párrafo anterior

5. En todo caso, bajo la supervisión de los responsables de la seguridad y de los responsables de la custodia y gestión del archivo electrónico y de los responsables de las unidades productoras de la documentación se establecerán los planes y se habilitarán los medios tecnológicos para la migración de los datos a otros formatos y soportes que permitan garantizar la autenticidad, integridad, disponibilidad, conservación y acceso al documento cuando el formato de los mismos deje de figurar entre los admitidos por el Esquema Nacional de Interoperabilidad y normativa correspondiente.

Artículo 55. *Archivo electrónico único.*

1. El archivo electrónico único de cada Administración es el conjunto de sistemas y servicios que sustenta la gestión, custodia y recuperación de los documentos y expedientes electrónicos así como de otras agrupaciones documentales o de información una vez finalizados los procedimientos administrativos o actuaciones correspondientes.

2. En el archivo electrónico único de la Administración General del Estado serán accesibles todos los documentos y expedientes electrónicos del sector público estatal una vez finalizados los procedimientos y en los plazos determinados por la Comisión Superior Calificadora de Documentos Administrativos de acuerdo con lo que se desarrolle reglamentariamente.

La gestión del archivo electrónico único garantizará la autenticidad, conservación, integridad, confidencialidad, disponibilidad y cadena de custodia de los expedientes y documentos almacenados, así como su acceso, en las condiciones exigidas por el Esquema Nacional de Interoperabilidad y el Esquema Nacional de Seguridad, por la normativa de transparencia, acceso a la información pública y buen gobierno, por la legislación de archivos y patrimonio histórico y cultural y por la normativa específica que sea de aplicación, de acuerdo con lo que se desarrolle reglamentariamente.

TÍTULO IV

De las relaciones y colaboración entre las Administraciones Públicas para el funcionamiento del sector público por medios electrónicos

CAPÍTULO I

Colaboración entre las Administraciones Públicas para la actuación administrativa por medios electrónicos

Artículo 56. *Relaciones interadministrativas e interorgánicas por medios electrónicos.*

De acuerdo con lo previsto en el artículo 3.2 de la Ley 40/2015, de 1 de octubre, las Administraciones Públicas, en el ejercicio de sus competencias, estarán obligadas a

relacionarse a través de medios electrónicos entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes.

Esta misma obligación será de aplicación a las entidades de derecho privado vinculadas o dependientes de las Administraciones públicas cuando actúen en el ejercicio de potestades administrativas.

Artículo 57. *Comunicaciones en la Administración General del Estado.*

Los órganos de la Administración General del Estado y los organismos públicos y entidades de derecho público vinculados o dependientes de esta deberán utilizar medios electrónicos para comunicarse entre sí.

Las comunicaciones se efectuarán a través del Registro Electrónico General de la Administración General del Estado o registro del organismo público o entidad de derecho público de que se trate, o por cualquier otro medio electrónico que permita dejar constancia de su recepción.

Esta misma obligación será de aplicación a las entidades de derecho privado vinculadas o dependientes de las Administraciones públicas cuando actúen en el ejercicio de potestades administrativas.

Artículo 58. *Adhesión a sedes electrónicas y sedes electrónicas asociadas.*

Las Administraciones Públicas y los organismos públicos y entidades de derecho público vinculados o dependientes podrán adherirse voluntariamente, mediante la formalización del correspondiente instrumento de adhesión, a las sedes electrónicas o sedes asociadas disponibles de titularidad de la misma Administración u otra Administración Pública, sin que se constituya como sede electrónica asociada.

Artículo 59. *Adhesión a la Carpeta Ciudadana del sector público estatal.*

Las Administraciones Públicas podrán integrar sus respectivas áreas personalizadas o carpetas ciudadanas a que se refiere el segundo párrafo del artículo 7.3 de este Reglamento, si las hubiere, o determinadas funcionalidades de las mismas, con la Carpeta Ciudadana prevista en el artículo 8 de este Reglamento, de forma que el interesado pueda acceder a sus contenidos o funcionalidades mediante procedimientos seguros que garanticen la integridad y confidencialidad de sus datos de carácter personal, independientemente de cuál haya sido su punto de acceso.

Artículo 60. *Sistema de interconexión de Registros.*

1. Las aplicaciones o sistemas de información para el tratamiento del Registro Electrónico General de cada Administración, así como del registro electrónico de cada organismo público o entidad de derecho público vinculado o dependiente, deberán ser interoperables.

2. Las interconexiones entre Registros de las Administraciones Públicas deberán realizarse a través del Sistema de Interconexión de Registros (SIR) gestionado por el Ministerio de Asuntos Económicos y Transformación Digital en colaboración con el Ministerio de Política Territorial y Función Pública de acuerdo con lo previsto en el Esquema Nacional de Interoperabilidad y en la correspondiente Norma Técnica.

3. En el ámbito de la Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes las aplicaciones o sistemas de información para el tratamiento del Registro Electrónico General de la Administración General del Estado, así como del registro electrónico de cada organismo público o entidad de derecho público vinculado o dependiente, deberán permitir la interoperabilidad con los sistemas de gestión de expedientes de las unidades de tramitación correspondientes.

Artículo 61. *Transmisiones de datos.*

1. Las transmisiones de datos a las que se refiere el artículo 155 de la Ley 40/2015, de 1 de octubre, realizadas a través de redes corporativas de las Administraciones Públicas para el envío de documentos elaborados por cualquier Administración, mediante consulta a las

plataformas de intermediación de datos u otros sistemas electrónicos habilitados al efecto, tienen la consideración de certificados administrativos necesarios para el procedimiento o actuación administrativa.

2. Cuando las personas interesadas no aporten datos y/o documentos que ya obren en poder de las Administraciones Públicas, de conformidad con lo establecido en la Ley 39/2015, de 1 de octubre, se seguirán las siguientes reglas:

a) Si el órgano administrativo encargado de la tramitación del procedimiento, puede acceder electrónicamente a los datos, documentos o certificados necesarios mediante consulta a las plataformas de intermediación de datos u otros sistemas electrónicos habilitados al efecto, los incorporará al procedimiento administrativo correspondiente. Quedará constancia en los ficheros del órgano, organismo público o entidad de derecho público cedente del acceso a los datos o documentos efectuado por el órgano u organismo cesionario.

b) Excepcionalmente, en caso de que no se pueda realizar el acceso electrónico a los datos mediante la consulta a que se refiere la letra anterior, se podrá solicitar por otros medios habilitados al efecto y se conservará la documentación acreditativa de la circunstancia que imposibilitó dicho acceso electrónico, incorporándola al expediente.

3. Toda transmisión de datos se efectuará a solicitud del órgano o entidad tramitadora en la que se identificarán los datos requeridos y sus titulares, así como la finalidad para la que se requieren. Además, si en la petición de datos interviene un empleado o empleada público se incluirá la identificación de este en la petición.

4. El órgano, organismo público o entidad de derecho público cesionario será responsable del correcto acceso electrónico a los datos cuya titularidad corresponda a otro órgano, organismo público o entidad de derecho público, así como de su utilización, en particular, cuando los datos a los que se accede tengan un régimen de especial protección. Asimismo, cuando para dicho acceso se requiera el consentimiento del interesado, el cesionario será responsable del requerimiento de dicho consentimiento.

5. La cesión de datos dentro de una actuación administrativa podrá llevarse a cabo, entre otras formas, de manera automatizada, entendiéndose por tal la consulta realizada íntegramente a través de medios telemáticos en la que no haya intervenido de forma directa un empleado o empleada público.

6. Las transmisiones de datos que se realicen en virtud del artículo 14 del Reglamento (UE) n.º 2018/1724 del Parlamento Europeo y del Consejo, de 2 de octubre de 2018, relativo a la creación de una pasarela digital única de acceso a información, procedimientos y servicios de asistencia y resolución de problemas y por el que se modifica el Reglamento (UE) n.º 1024/2012 no requerirán previsualización de los datos por parte del usuario o usuaria solicitante para proceder a su uso por parte del órgano o entidad tramitadora.

Artículo 62. *Plataformas de intermediación de datos.*

1. Las plataformas de intermediación de datos dejarán constancia de la fecha y hora en que se produjo la transmisión, así como del procedimiento administrativo, trámite o actuación al que se refiere la consulta. Las plataformas de intermediación, o sistema electrónico equivalente, existentes en el sector público deberán ser interoperables con la Plataforma de Intermediación de la Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes y entre ellas.

La adhesión a las plataformas de intermediación de datos requerirá que se garantice el cumplimiento de las condiciones de seguridad exigidas por los cedentes de la información para el tratamiento de datos por parte de la plataforma encargada del tratamiento de dichos datos y de los cesionarios de los mismos.

2. En el ámbito estatal, se dispondrá de la Plataforma de Intermediación de Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes a que se refiere la Ley 39/2015, de 1 de octubre. Dicha Plataforma será gestionada la Secretaría General de Administración Digital y actuará como un punto a través del cual cualquier órgano, organismo público o entidad de derecho público podrá consultar los datos o documentos asociados al procedimiento de que se trate, con

independencia de que la presentación de los citados datos o documentos tenga carácter preceptivo o facultativo en el procedimiento de que se trate.

3. La Plataforma de Intermediación de la Administración General del Estado actuará como punto de conexión con el sistema técnico regulado por el Reglamento (UE) n.º 2018/1724 del Parlamento Europeo y del Consejo, de 2 de octubre de 2018, para el intercambio automático de datos o documentos a nivel europeo.

Artículo 63. *Remisión electrónica de expedientes administrativos en el ámbito de las Administraciones públicas mediante puesta a disposición.*

1. Cuando desde una Administración Pública se solicite a otra un expediente electrónico, la remisión por esta, a través de un nodo de interoperabilidad, de la dirección electrónica o localizador que dé acceso al expediente electrónico puesto a disposición de la primera equivaldrá a la remisión del mismo, siempre que se garantice la integridad del acceso a lo largo del tiempo que determine la correspondiente política de gestión de documentos electrónicos y el cumplimiento de la normativa de interoperabilidad aplicable al tipo de expediente.

2. El mismo procedimiento previsto en el apartado anterior se podrá utilizar cuando la solicitud se produzca dentro del ámbito de una misma Administración Pública.

CAPÍTULO II

Transferencia y uso compartido de tecnologías entre Administraciones Públicas

Artículo 64. *Reutilización de sistemas y aplicaciones de las Administraciones Públicas.*

1. De acuerdo con lo previsto en el artículo 157 de la Ley 40/2015, de 1 de octubre, las Administraciones Públicas pondrán a disposición de cualquiera de ellas que lo solicite las aplicaciones, desarrolladas por sus servicios o que hayan sido objeto de contratación y de cuyos derechos de propiedad intelectual sean titulares, salvo que la información a la que estén asociadas sea objeto de especial protección por estar previsto en una norma. Las Administraciones cedentes y cesionarias podrán acordar la repercusión del coste de adquisición o fabricación de las aplicaciones cedidas.

2. A tal efecto, de acuerdo con lo previsto en el artículo 158 de la Ley 40/2015, de 1 de octubre, las Administraciones Públicas mantendrán directorios actualizados de aplicaciones para su libre reutilización en modo producto o en modo servicio, de conformidad con lo dispuesto en el Esquema Nacional de Interoperabilidad.

Estos directorios deberán ser plenamente interoperables, de modo que se garantice su compatibilidad informática e interconexión, con el Directorio general de aplicaciones de la Administración General del Estado para su libre reutilización previsto en el artículo 17 del Real Decreto 4/2010, de 8 de enero.

3. Las condiciones de licenciamiento de los sistemas y aplicaciones de las Administraciones públicas y el uso y funcionamiento de los directorios de aplicaciones reutilizables deberán ajustarse a lo previsto en el Real Decreto 4/2010, de 8 de enero.

4. Las Administraciones públicas procurarán la construcción de aplicaciones reutilizables, bien en modo producto o en modo servicio, con el fin de favorecer las actuaciones de compartir, reutilizar y colaborar, en beneficio de una mejor eficiencia y para atender de forma efectiva las solicitudes recibidas en virtud del artículo 157 de la Ley 40/2015, de 1 de octubre.

5. Las Administraciones Públicas, con carácter previo a la adquisición, desarrollo o al mantenimiento a lo largo de todo el ciclo de vida de una aplicación, tanto si se realiza con medios propios o por la contratación de los servicios correspondientes, deberán consultar en el Directorio general de aplicaciones de la Administración General del Estado para su libre reutilización, si existen soluciones disponibles para su reutilización, que puedan satisfacer total o parcialmente las necesidades, mejoras o actualizaciones que se pretenden cubrir, y siempre que los requisitos tecnológicos de interoperabilidad y seguridad así lo permitan.

Las conclusiones con respecto al resultado de dicha consulta al directorio general se incorporarán en el expediente de contratación y reflejarán, en su caso, que no existen

soluciones disponibles para su reutilización que puedan satisfacer total o parcialmente las necesidades, mejoras o actualizaciones que se pretenden cubrir.

En el caso de existir una solución disponible para su reutilización total o parcial, la justificación de la no reutilización se realizará en términos de eficiencia conforme a lo establecido en el artículo 7 de la Ley Orgánica 2/2012, de 27 de abril, de Estabilidad Presupuestaria y Sostenibilidad Financiera.

Artículo 65. *Adhesión a las plataformas de la Administración General del Estado.*

1. La adhesión al uso de las plataformas, registros o servicios electrónicos de la Administración General del Estado prevista en la Ley 39/2015, de 1 de octubre, en la Ley 40/2015, de 1 de octubre, y en este Reglamento, así como a aquellos otros que puedan facilitar el cumplimiento de lo dispuesto en estas normas se realizará mediante adhesión por el órgano competente de la Administración Pública que corresponda, en el que se dejará constancia de la voluntad de este de adherirse a las plataformas, registros o servicios electrónicos y de aceptar en su integridad las condiciones de uso determinadas por el órgano titular de la plataforma o servicio, incluyendo el comienzo efectivo del mismo.

A tal efecto, los modelos de adhesión a las plataformas, registros o servicios, que incluirán los términos de prestación del servicio y de la contribución al sostenimiento del mismo, se aprobarán mediante Resolución de la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital o, en su caso, del órgano directivo, organismo público o entidad de derecho público que sea competente de las plataformas, registros o servicios de que se trate.

2. La adhesión a una plataforma, registro o servicio electrónico de la Administración General del Estado no supondrá un cambio de la titularidad sobre las actuaciones administrativas realizadas en el procedimiento administrativo de que se trate, que corresponderá a la Administración competente para su tramitación. Si la plataforma provee un servicio que requiere el intercambio de información entre dos entidades usuarias de la misma o de distinta plataforma, la autenticación de la entidad solicitante puede acreditarse, ante la entidad cedente, mediante un sello electrónico cualificado del órgano, organismo público o entidad de derecho público que gestiona la plataforma en cuestión de la que es usuaria la entidad solicitante, que actuará en nombre de los órganos y organismos o entidades adheridos que actúan como solicitantes.

La adhesión a una plataforma de la Administración General del Estado requerirá que se cumplan las condiciones de seguridad exigidas por los cedentes de la información.

3. Los órganos competentes para la gestión del procedimiento administrativo de las Administraciones que se adhieran a estas plataformas, registros o servicios electrónicos se responsabilizarán del uso que hagan de las mismas en el ejercicio de sus competencias, correspondiendo al órgano responsable de la plataforma su gestión y mantenimiento. En el supuesto de que una incidencia técnica imposibilite el funcionamiento ordinario del sistema o aplicación que corresponda, y sin perjuicio de la ampliación de plazos a que se refiere el artículo 32.4 de la Ley 39/2015, de 1 de octubre, cada Administración pública será responsable de la continuación de la tramitación de sus procedimientos administrativos y servicios a la ciudadanía.

4. La adhesión de las comunidades autónomas o entidades locales a las plataformas estatales o registros previstos en la disposición adicional segunda de la Ley 39/2015, de 1 de octubre, es voluntaria, si bien la no adhesión deberá justificarse en términos de eficiencia conforme al artículo 7 de la Ley Orgánica 2/2012, de 27 de abril, de Estabilidad Presupuestaria y Sostenibilidad Financiera, para lo que se enviará el correspondiente informe al Ministerio de Asuntos Económicos y Transformación Digital, en el que deberá incluirse la justificación del cumplimiento de los requisitos del Esquema Nacional de Interoperabilidad, el Esquema Nacional de Seguridad y sus normas técnicas de desarrollo, de plataformas, registros o servicios electrónicos que se utilicen, de modo que se garantice su compatibilidad informática e interconexión, así como la transmisión telemática de las solicitudes, escritos y comunicaciones que se realicen en sus correspondientes plataformas.

Disposición adicional primera. *Obligatoriedad de uso de medios electrónicos en los procesos selectivos para el acceso al empleo público en el ámbito de la Administración General del Estado.*

Las personas participantes en procesos selectivos convocados por la Administración General del Estado, sus organismos públicos o entidades de derecho público vinculados o dependientes a la misma, deberán realizar la presentación de las solicitudes y documentación y, en su caso, la subsanación y los procedimientos de impugnación de las actuaciones de estos procesos selectivos a través de medios electrónicos.

Disposición adicional segunda. *Formación de empleados y empleadas públicos de la Administración General del Estado.*

La Administración General del Estado promoverá la formación del personal a su servicio para garantizar el derecho de las personas interesadas a ser asistidas en el uso de medios electrónicos en sus relaciones con la Administración Pública, establecido en la Ley 39/2015, de 1 de octubre.

Disposición adicional tercera. *Nodo de interoperabilidad de identificación electrónica del Reino de España.*

1. Se crea el nodo de interoperabilidad de identificación electrónica del Reino de España para el reconocimiento mutuo de identidades electrónicas entre los Estados miembros, de acuerdo con lo previsto en el Reglamento (UE) n.º 910/2014, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

2. El nodo de interoperabilidad de identificación electrónica del Reino de España se gestionará por el Ministerio de Asuntos Económicos y Transformación Digital.

3. Las entidades pertenecientes al sector público deberán definir y publicar en su sede electrónica el nivel de seguridad en la identificación electrónica exigido en los procedimientos y servicios que gestionan, de acuerdo con el Reglamento (UE) n.º 910/2014, de 23 de julio de 2014. Este nivel de seguridad en la identificación electrónica del sistema de información que soporta el procedimiento o servicio se determinará sobre la base del análisis de riesgos, de acuerdo con el Esquema Nacional de Seguridad y normativa correspondiente.

4. Las entidades pertenecientes al sector público deberán admitir en todo caso, en el acceso electrónico a sus procedimientos y servicios los esquemas de identificación notificados por otros Estados Miembros al amparo del Reglamento (UE) n.º 910/2014, de 23 de julio de 2014, siempre que se den estas dos condiciones:

a) El esquema de identificación utilizado tenga un nivel de seguridad en la identificación electrónica sustancial o alto.

b) El nivel de seguridad de dicho esquema sea igual o superior al nivel de seguridad exigido por el procedimiento o servicio de acuerdo con el apartado 3.

Disposición adicional cuarta. *Adhesión de las entidades de derecho privado vinculadas o dependientes de la Administración General del Estado en el ejercicio de potestades administrativas a las sedes electrónicas y sedes electrónicas asociadas y sistema de firma y notificaciones electrónicas aplicables.*

De acuerdo con lo previsto en el artículo 2.2.b) de la Ley 39/2015, de 1 de octubre, y el artículo 2.2.b) de la Ley 40/2015, de 1 de octubre, cuando las entidades de derecho privado vinculadas o dependientes de la Administración General del Estado ejerzan potestades administrativas y, en consecuencia, les sea de aplicación este Reglamento, se observarán las siguientes disposiciones:

a) De acuerdo con lo previsto en el artículo 58, las entidades de derecho privado tendrán que adherirse a la sede electrónica asociada del ministerio con el que mantengan la vinculación o dependencia o, en su caso, a la sede electrónica o sede electrónica asociada del organismo de derecho público con el que mantengan la misma, en ambos casos mediante la formalización del correspondiente instrumento de adhesión.

Las personas interesadas obligadas a relacionarse electrónicamente con las entidades de derecho privado en el ejercicio de dichas potestades realizarán los trámites del procedimiento mediante los modelos normalizados que estarán disponibles en la sede electrónica asociada o, en su caso, sede electrónica a la que se haya adherido la entidad. El mismo régimen se aplicará a los sujetos no obligados que hayan optado por medios electrónicos de acuerdo con lo previsto en el artículo 3 de este Reglamento.

b) Según lo previsto en los artículos 20.2 y 22.4, mediante orden de la persona titular del Ministerio de Asuntos Económicos y Transformación Digital se determinarán reglamentariamente los medios admitidos para la firma electrónica en los procedimientos tramitados en el ejercicio de potestades administrativas por parte de las entidades de derecho privado vinculadas o dependientes de la Administración General del Estado.

c) De conformidad con lo previsto en el artículo 42, las notificaciones electrónicas que las entidades de derecho privado tengan que practicar se llevarán a cabo en la misma forma que el responsable de la sede electrónica asociada o sede electrónica a la que esté adherida la entidad haya dispuesto para sus propias notificaciones.

Disposición adicional quinta. *Adhesión de los órganos constitucionales al uso de las plataformas, registros o servicios electrónicos de la Administración General del Estado.*

1. Sin perjuicio de lo previsto en el artículo 65 de este Reglamento, los órganos constitucionales podrán adherirse al uso de las plataformas, registros o servicios electrónicos de la Administración General del Estado y aquellos otros que puedan facilitar el cumplimiento de lo dispuesto en la Ley 39/2015, de 1 de octubre, en la Ley 40/2015, de 1 de octubre, y en este Reglamento.

2. La adhesión se realizará mediante un acuerdo o acto de adhesión en el que la autoridad competente de las instituciones u órganos anteriores dejará constancia de la voluntad de este de adherirse a las plataformas, registros o servicios electrónicos y de aceptar en su integridad las condiciones de uso determinadas por el órgano titular de la plataforma o servicio, incluyendo el comienzo efectivo del mismo.

Para el estudio de su viabilidad, remitirá con carácter previo al Ministerio al que pertenezca el órgano titular de la plataforma o servicio una memoria justificativa y económica en que se explicite el volumen de trámites que estaría previsto realizar a través de la plataforma, el registro o servicio electrónico de que se trate, los efectos presupuestarios y económicos y cualquier otra razón de interés general que justifique su adhesión.

3. La adhesión a una plataforma, registro o servicio electrónico de la Administración General del Estado no supondrá un cambio de la titularidad sobre las actuaciones administrativas realizadas en el procedimiento administrativo de que se trate, que corresponderá a la Administración competente para su tramitación.

Si la plataforma, registro o servicio electrónico provee un servicio que requiere el intercambio de información entre dos entidades usuarias de la misma o distinta plataforma, la autenticación de la entidad solicitante puede acreditarse ante la entidad cedente mediante un sello electrónico cualificado del órgano, organismo público o entidad de derecho público que gestiona la plataforma.

4. La adhesión a una plataforma de la Administración General del Estado requerirá que se cumplan las condiciones de seguridad exigidas por los cedentes de la información.

5. Los órganos competentes en las instituciones u órganos adheridos se responsabilizarán del uso que hagan de las plataformas en el ejercicio de sus competencias, correspondiendo al órgano responsable de la plataforma su gestión y mantenimiento. En el supuesto de una incidencia técnica imposibilite el funcionamiento ordinario del sistema o aplicación que corresponda, los órganos competentes en las instituciones u órganos adheridos serán responsables de la continuación de la tramitación de sus procedimientos administrativos.

Disposición adicional sexta. *Situación de las sedes electrónicas y subsedes electrónicas en el ámbito estatal existentes a la entrada en vigor de este real decreto.*

1. En aplicación de lo previsto en el artículo 38 de la Ley 40/2015, de 1 de octubre, las sedes electrónicas existentes en la Administración General del Estado en la fecha de entrada en vigor de este real decreto pasan a tener naturaleza de sedes electrónicas

asociadas de la sede electrónica de la Administración General del Estado, que es la sede del Punto de Acceso General electrónico (PAGe) de la Administración General del Estado, sin necesidad de modificar su instrumento de creación. Las subsedes electrónicas existentes en la fecha de entrada en vigor de este real decreto pasarán también a tener naturaleza de sedes electrónicas asociadas.

2. Las sedes electrónicas de los organismos públicos o entidades de derecho público vinculados o dependientes existentes en la fecha de entrada en vigor de este real decreto mantendrán su naturaleza de sede electrónica. Las subsedes electrónicas de estos pasarán a tener naturaleza de sedes electrónicas asociadas.

Disposición adicional séptima. *Interoperabilidad de los registros electrónicos de apoderamientos.*

1. En aplicación de lo previsto en el artículo 6 de la Ley 39/2015, de 1 de octubre, y el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica, la Norma Técnica de Interoperabilidad establecerá el modelo de datos y las condiciones de interoperabilidad de los registros electrónicos de apoderamientos, abordando los aspectos funcionales y técnicos para la plena interoperabilidad de los registros electrónicos de apoderamientos pertenecientes a las Administraciones, así como la interconexión de estos a las sedes electrónicas, a los registros mercantiles, de la propiedad y a los protocolos notariales.

2. En el ámbito de la Administración General del Estado, el cumplimiento de las previsiones del artículo 33.2 del Reglamento sobre el acceso al Registro Electrónico de Apoderamientos de la Administración General del Estado está vinculado a la aprobación y aplicación de la Norma Técnica a que se refiere el apartado 1 anterior.

Disposición adicional octava. *Supletoriedad en Registro Civil.*

De conformidad con lo dispuesto en el artículo 88 y en la Disposición final primera de la Ley 20/2011, de 21 de julio, del Registro Civil, este Reglamento será de aplicación supletoria en lo no previsto en dicha Ley y su normativa de desarrollo específica, en cuanto a todo lo relacionado con la tramitación administrativa de los procedimientos específicos de Registro Civil.

Disposición adicional novena. *Autorización de los sistemas de identificación previstos en el artículo 9.2.c) y de los sistemas de firma previstos en el artículo 10.2.c) de la Ley 39/2015, de 1 de octubre.*

1. Los sistemas de identificación a que se refiere el artículo 9.2.c) y los sistemas de firma a que se refiere el artículo 10.2.c) de la ley 39/2015, de 1 de octubre, que, en ambos casos, se hubieran puesto en servicio hasta el 6 de noviembre de 2019, fecha de entrada en vigor de la modificación de dichos artículos en virtud del Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones, no requerirán la autorización de la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital, previo informe vinculante de la Secretaría de Estado de Seguridad del Ministerio del Interior, siempre y cuando no hayan sido modificados tras dicha fecha.

2. Los sistemas que, tras el 6 de noviembre de 2019, hayan sido autorizados en aplicación de las previsiones de los artículos 9.2.c) y 10.2.c) de la Ley 39/2015, de 1 de octubre, y sean modificados posteriormente, deberán ser objeto de una nueva autorización previa a su puesta en servicio.

Disposición adicional décima. *Especialidades por razón de materia.*

1. De acuerdo con la disposición adicional primera de la Ley 39/2015, de 1 de octubre, los procedimientos administrativos regulados en leyes especiales por razón de la materia que no exijan alguno de los trámites previstos en la citada ley o regulen trámites adicionales o distintos se regirán, respecto a estos, por lo dispuesto en dichas leyes especiales.

2. Las siguientes actuaciones y procedimientos se regirán por su normativa específica y supletoriamente por lo dispuesto en la Ley 39/2015, de 1 de octubre:

a) Las actuaciones y procedimientos de aplicación de los tributos en materia tributaria y aduanera, así como su revisión en vía administrativa.

b) Las actuaciones y procedimientos de gestión, inspección, liquidación, recaudación, impugnación y revisión en materia de Seguridad Social y desempleo.

c) Las actuaciones y procedimientos sancionadores en materia tributaria y aduanera, en el orden social, en materia de tráfico y seguridad vial y en materia de extranjería.

d) Las actuaciones y procedimientos en materia de extranjería y asilo.

3. De acuerdo con lo previsto en la Disposición adicional decimoséptima de la Ley 40/2015, de 1 de octubre, la Agencia Estatal de Administración Tributaria se regirá por su legislación específica y únicamente de forma supletoria y en tanto resulte compatible con su legislación específica por lo previsto en dicha Ley. El acceso, la cesión o la comunicación de información de naturaleza tributaria se regirán en todo caso por su legislación específica.

ANEXO

Definiciones

– Aplicación de fuentes abiertas: Aquella que se distribuye con una licencia que permite la libertad de ejecutarla, de conocer el código fuente, de modificarla o mejorarla y de redistribuir copias a otras personas usuarias.

– Archivo electrónico único de cada Administración: Conjunto de sistemas y servicios que sustente la gestión, custodia y recuperación de los documentos y expedientes electrónicos así como de otras agrupaciones documentales o de información una vez finalizados los procedimientos o actuaciones correspondientes.

– Autenticación: Procedimiento de verificación de la identidad digital de un sujeto en sus interacciones en el ámbito digital, típicamente mediante factores tales como «algo que se sabe»(contraseñas o claves concertadas), «algo que se tiene» sean componentes lógicos (como certificados software) o dispositivos físicos (en expresión inglesa, tokens), o «algo que se es» (elementos biométricos), factores utilizados de manera aislada o combinados.

– Autenticidad: Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

– Canal: Estructura o medio de difusión de los contenidos y servicios; incluyendo el canal presencial, el telefónico y el electrónico, así como otros que existan en la actualidad o puedan existir en el futuro (dispositivos móviles, etc.).

– Certificado electrónico: Documento emitido y firmado por la Autoridad de Certificación que identifica una clave pública con su propietario. Cada certificado está identificado por un número de serie único y tiene un periodo de validez que está incluido en el certificado.

– Certificado cualificado: Un certificado de firma electrónica que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo I del Reglamento UE 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones, electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

– Certificado cualificado de sello electrónico: Certificado de sello electrónico que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo III del Reglamento UE 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones, electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE

– Código malicioso: Tipo de software de carácter dañino que crea o aprovecha vulnerabilidades en dispositivos, sistemas y archivos informáticos que permiten el acceso remoto no autorizado, la generación de puertas traseras, el robo o exfiltración de datos, la destrucción de información, u otras acciones perjudiciales.

– Código Seguro de Verificación (CSV): Código que identifica a un documento electrónico y cuya finalidad es garantizar el origen e integridad de los documentos mediante

el acceso a la sede electrónica correspondiente; el carácter único del código generado para cada documento; su vinculación con el documento generado, de forma que cualquier modificación del documento generado dará lugar a un nuevo documento con un código seguro de verificación diferente; la posibilidad de verificar el documento en la sede electrónica como mínimo por el tiempo que se establezca en la resolución que autorice la aplicación de este procedimiento; así como un acceso al documento restringido a quien disponga del código seguro de verificación.

– Confidencialidad: Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

– Copia auténtica: Tendrá la consideración de copia auténtica de un documento público administrativo o privado original o de otra copia auténtica, la realizada, cualquiera que sea su soporte, por los órganos competentes de las Administraciones Públicas en las que quede garantizada la identidad del órgano que ha realizado la copia y su contenido

– Copia autorizada electrónica: documento notarial electrónico generado por el notario que autorizó la escritura, con el mismo valor y efectos que la copia en papel y al cual se le atribuye también valor de documento público.

– Digitalización: Proceso tecnológico que permite convertir un documento en soporte papel o en otro soporte no electrónico en uno o varios ficheros electrónicos que contienen la imagen codificada, fiel e íntegra del documento.

– Dirección electrónica: Identificador de un equipo o sistema electrónico desde el que se provee de información o servicios en una red de comunicaciones

– Directorio de aplicaciones reutilizables: instrumento que contiene la relación de aplicaciones para su libre reutilización, incluyendo, al menos, los datos descriptivos relativos a nombre de la aplicación, breve descripción de sus funcionalidades, uso y características, licencia, principales estándares abiertos aplicados, y estado de desarrollo.

– Disponibilidad: Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

– Documento electrónico: Información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado.

– Entorno cerrado de comunicación: escenario de comunicaciones delimitado, controlado y protegido en el que los participantes se relacionan a través de medios electrónicos, según unas garantías y condiciones determinadas que incluyen la relación de emisores y receptores autorizados, la naturaleza de los datos a intercambiar y las medidas de seguridad y protección de datos.

– Especificación técnica: Según el Reglamento n.º 1025/2012, del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, sobre normalización europea, documento en el que se prescriben los requisitos técnicos que debe reunir un producto, proceso, servicio o sistema y que establece uno o más de los aspectos siguientes:

• Las características que debe tener un producto, como los niveles de calidad, rendimiento, interoperabilidad, protección del medio ambiente, salud y seguridad y sus dimensiones, así como los requisitos aplicables al producto en lo que respecta a la denominación con la que se vende, la terminología, los símbolos, los ensayos y los métodos de ensayo, el embalaje, el marcado o el etiquetado y los procedimientos de evaluación de la conformidad;

• los métodos y procedimientos de producción de los productos agrícolas, definidos en el artículo 38, apartado 1, del TFUE, de los productos destinados a la alimentación humana y animal y de los medicamentos, así como los métodos y procedimientos de producción relacionados con los demás productos, en caso de que estos influyan en sus características;

• las características que debe tener un servicio, como los niveles de calidad, rendimiento, interoperabilidad, protección del medio ambiente, salud o seguridad, así como los requisitos aplicables al proveedor en lo que respecta a la información que debe facilitarse a la persona destinataria, tal como se especifica en el artículo 22, apartados 1 a 3, de la Directiva 2006/123/CE del Parlamento Europeo y del Consejo de 12 de diciembre de 2006 relativa a los servicios en el mercado interior.

• los métodos y los criterios para evaluar el rendimiento de los productos de construcción, tal como se definen en el artículo 2, punto 1, del Reglamento (UE) n.º 305/2011

del Parlamento Europeo y del Consejo, de 9 de marzo de 2011, por el que se establecen condiciones armonizadas para la comercialización de productos de construcción, en relación con sus características esenciales.

– Esquema Nacional de Interoperabilidad: Instrumento que comprende el conjunto de criterios y recomendaciones en materia de seguridad, conservación y normalización de la información, de los formatos y de las aplicaciones que deberán ser tenidos en cuenta por las Administraciones Públicas para la toma de decisiones tecnológicas que garanticen la interoperabilidad.

– Esquema Nacional de Seguridad: Instrumento que tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada.

– Expediente administrativo: Conjunto ordenado de documentos y actuaciones relativos a la resolución administrativa, así como las diligencias encaminadas a ejecutarla.

– Firma electrónica: Los datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar.

– Firma electrónica avanzada: La firma electrónica que cumple los requisitos contemplados en el artículo 26 del Reglamento eIDAS.

– Firma electrónica cualificada: Una firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica.

– Formato de documento: Conjunto de reglas (algoritmo) que define la manera correcta de intercambiar o almacenar datos en memoria. Se corresponde habitualmente con una especificación técnica.

– Identificación: Procedimiento para reconocer de forma única la identidad de un sujeto que culmina tras un registro previo con la asignación de un elemento identificador singular en formato electrónico que representa de forma única a una persona física o jurídica o a una persona física que representa a una persona jurídica para interacción en el entorno digital.

– Infraestructura o servicio común: Capacidad organizativa y técnica que satisface necesidades comunes de las personas usuarias en diversos ámbitos de la Administración, junto con su gobernanza operativa de apoyo, que pueden tener carácter horizontal o sectorial, con diversos modos de provisión, como servicio o como producto, o integración a modo de plataforma, que facilitan la interoperabilidad, la seguridad, las economías de escala, la racionalización y la simplificación de la actuación administrativa.

– Integridad: Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.

– Interoperabilidad: Capacidad de los sistemas de información, y por ende de los procedimientos a los que estos dan soporte, de compartir datos y posibilitar el intercambio de información entre ellos.

– Licenciamiento: Condiciones aplicables a la reutilización de cualquier tipo de material en formato electrónico que pueda ser empleado de forma recurrente.

– Marca de tiempo: La asignación por medios electrónicos de la fecha y, en su caso, la hora a un documento electrónico.

– Metadato: Dato que define y describe otros datos. Existen diferentes tipos de metadatos según su aplicación.

– Metadato de gestión de documentos: Información estructurada o semiestructurada que hace posible la creación, gestión y uso de documentos a lo largo del tiempo en el contexto de su creación. Los metadatos de gestión de documentos sirven para identificar, autenticar y contextualizar documentos, y del mismo modo a las personas, los procesos y los sistemas que los crean, gestionan, mantienen y utilizan.

– Nodo de interoperabilidad: Entidad que presta servicios de interconexión técnica, organizativa y jurídica entre sistemas de información para un conjunto de Administraciones Públicas bajo las condiciones que estas fijen.

– Política de firma electrónica: Conjunto de directrices y normas técnicas aplicables a la utilización de certificados y firma electrónica dentro de su ámbito de aplicación.

– Política de gestión de documentos electrónicos: Orientaciones o directrices que define una organización para la creación y gestión de documentos auténticos, fiables y disponibles a lo largo del tiempo, de acuerdo con las funciones y actividades que le son propias. La política se aprueba al más alto nivel dentro de la organización, y asigna responsabilidades en cuanto a la coordinación, aplicación, supervisión y gestión del programa de tratamiento de los documentos a través de su ciclo de vida.

– Portal de internet de una Administración Pública: Se entiende por portal de internet el punto de acceso electrónico cuya titularidad corresponda a una Administración Pública, organismo público o entidad de derecho público que permite el acceso a través de internet a la información publicada y, en su caso, a la sede electrónica correspondiente.

– Prestador de Servicios de Confianza: Persona física o jurídica que presta uno o más servicios de confianza, bien como prestador cualificado o como prestador no cualificado de servicios de confianza, según lo previsto en el Reglamento eIDAS.

– Punto de Acceso General: Portal de internet que facilita el acceso a los servicios, trámites e información de los órganos, organismos públicos y entidades vinculados o dependientes de la Administración Pública correspondiente y aglutina o conduce a las sedes electrónicas asociadas de sus órganos y las sedes electrónicas de sus organismos públicos y entidades de derecho público.

– Sello electrónico: Datos en formato electrónico anejos a otros datos en formato electrónico, o asociados de manera lógica con ellos, para garantizar el origen y la integridad de estos últimos.

– Sello electrónico avanzado: Sello electrónico que cumple los siguientes requisitos: 1) estar vinculado al creador del sello de manera única; 2) permitir la identificación del creador del sello; 3) haber sido creado utilizando datos de creación del sello electrónico que el creador del sello puede utilizar para la creación de un sello electrónico, con un alto nivel de confianza, bajo su control, y 4) estar vinculado con los datos a que se refiere de modo tal que cualquier modificación ulterior de los mismos sea detectable.

– Sello electrónico cualificado: Sello electrónico avanzado que se crea mediante un dispositivo cualificado de creación de sellos electrónicos y que se basa en un certificado cualificado de sello electrónico.

– Sede electrónica: Dirección electrónica, disponible para la ciudadanía a través de redes de telecomunicaciones, cuya titularidad corresponde a una Administración Pública, o bien a uno o varios organismos públicos o entidades de derecho público en el ejercicio de sus competencias.

– Sede electrónica asociada: Sede electrónica disponible para la ciudadanía a través de redes de telecomunicaciones que se crea por razones organizativas o técnicas vinculada a la sede electrónica de una Administración Pública o a la sede electrónica de un organismo público o entidad de derecho público.

– Sello de tiempo: Asignación por medios electrónicos de una fecha y hora a un documento electrónico con la intervención de un prestador de servicios de certificación que asegure la exactitud e integridad de la marca de tiempo del documento

– Sistema de Interconexión de Registros: Infraestructura básica que permite el intercambio de asientos electrónicos de registro entre las Administraciones Públicas.

– Trazabilidad: Posibilidad de identificar el origen de un documento en las distintas fases de su producción, pudiendo determinar en qué fase y por quién se han producido, en su caso, las modificaciones del documento original.

§ 38

Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza

Jefatura del Estado
«BOE» núm. 298, de 12 de noviembre de 2020
Última modificación: 9 de mayo de 2023
Referencia: BOE-A-2020-14046

FELIPE VI

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley:

PREÁMBULO

I

Desde el 1 de julio de 2016 es de aplicación el Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.

La Ley 59/2003, de 19 de diciembre, de firma electrónica, que supuso la transposición al ordenamiento jurídico español de la derogada Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica, se encuentra desde entonces jurídicamente desplazada en todo aquello regulado por el citado Reglamento. El objeto de esta Ley es, por tanto, adaptar nuestro ordenamiento jurídico al marco regulatorio de la Unión Europea, evitando así la existencia de vacíos normativos susceptibles de dar lugar a situaciones de inseguridad jurídica en la prestación de servicios electrónicos de confianza.

La presente Ley no realiza una regulación sistemática de los servicios electrónicos de confianza, que ya han sido legislados por el Reglamento (UE) 910/2014, el cual, por respeto al principio de primacía del Derecho de la Unión Europea, no debe reproducirse total o parcialmente. La función de esta Ley es complementarlo en aquellos aspectos concretos que el Reglamento no ha armonizado y cuyo desarrollo prevé en los ordenamientos de los diferentes Estados miembros, cuyas disposiciones han de ser interpretadas de acuerdo con él.

II

En lugar de una revisión de la Directiva 1999/93/CE, la elección de un reglamento como instrumento legislativo por el legislador europeo, de aplicación directa en los Estados miembros, vino motivada por la necesidad de reforzar la seguridad jurídica en el seno de la Unión, terminando con la dispersión normativa provocada por las transposiciones de la citada Directiva en los ordenamientos jurídicos internos a través de leyes nacionales, que había provocado una importante fragmentación e imposibilitado la prestación de servicios transfronterizos en el mercado interior, agravada por las diferencias en los sistemas de supervisión aplicados en cada Estado miembro.

Así, mediante el Reglamento (UE) 910/2014 se persigue regular en un mismo instrumento normativo de aplicación directa en los Estados miembros dos realidades, la identificación y los servicios de confianza electrónicos en sentido amplio, armonizando y facilitando el uso transfronterizo de los servicios en línea, públicos y privados, así como el comercio electrónico en la UE, contribuyendo así al desarrollo del mercado único digital.

Por una parte, en el ámbito de la identificación electrónica, el Reglamento instaura la aceptación mutua, para el acceso a los servicios públicos en línea, de los sistemas nacionales de identificación electrónica que hayan sido notificados a la Comisión Europea por parte de los Estados miembros, con objeto de facilitar la interacción telemática segura con las Administraciones públicas y su utilización para la realización de trámites transfronterizos, eliminando esta barrera electrónica que excluía a los ciudadanos del pleno disfrute de los beneficios del mercado interior.

Por otra parte, introduce la regulación armónica de nuevos servicios electrónicos cualificados de confianza, adicionales a la tradicional firma electrónica, tales como el sello electrónico de persona jurídica, el servicio de validación de firmas y sellos cualificados, el servicio de conservación de firmas y sellos cualificados, el servicio de sellado electrónico de tiempo, el servicio de entrega electrónica certificada y el servicio de expedición de certificados de autenticación web, que pueden ser combinados entre sí para la prestación de servicios complejos e innovadores.

Se establece un régimen jurídico específico para los citados servicios electrónicos de confianza cualificados, consecuente con las elevadas exigencias de supervisión y seguridad que soportan, y cuyo reflejo es la singular relevancia probatoria que poseen respecto de los servicios no cualificados. Se refuerza así la seguridad jurídica de las transacciones electrónicas entre empresas, particulares y Administraciones públicas.

III

La aplicabilidad directa del Reglamento no priva a los Estados miembros de toda capacidad normativa sobre la materia regulada, es más, aquellos están obligados a adaptar los ordenamientos nacionales para garantizar que aquella cualidad se haga efectiva. Esta adaptación puede exigir tanto la modificación o derogación de normas existentes, como la adopción de nuevas disposiciones llamadas a completar la regulación europea.

En tal sentido, el objetivo de la presente Ley, como se indicaba ut supra, es complementar el Reglamento (UE) 910/2014 en aquellos aspectos que este no ha armonizado y que se dejan al criterio de los Estados miembros. Por tanto, la Ley se abstiene de reproducir las previsiones del Reglamento, abordando únicamente aquellas cuestiones que la norma europea remite a la decisión de los Estados miembros o que no se encuentran armonizadas, adquiriendo la regulación coherencia y sentido en el marco de la normativa europea.

Así, en virtud del principio de proporcionalidad, esta Ley contiene la regulación imprescindible para cubrir aquellos aspectos previstos en el Reglamento (UE) 910/2014, como es el caso, entre otros, del régimen de previsión de riesgo de los prestadores cualificados, el régimen sancionador, la comprobación de la identidad y atributos de los solicitantes de un certificado cualificado, la inclusión de requisitos adicionales a nivel nacional para certificados cualificados tales como identificadores nacionales, o su tiempo máximo de vigencia, así como las condiciones para la suspensión de los certificados.

El Reglamento (UE) 910/2014 garantiza la equivalencia jurídica entre la firma electrónica cualificada y la firma manuscrita, pero permite a los Estados miembros determinar los

efectos de las otras firmas electrónicas y de los servicios electrónicos de confianza en general. En este aspecto, se modifica la regulación anterior al atribuir a los documentos electrónicos para cuya producción o comunicación se haya utilizado un servicio de confianza cualificado una ventaja probatoria. A este respecto, se simplifica la prueba, pues basta la mera constatación de la inclusión del citado servicio en la lista de confianza de prestadores cualificados de servicios electrónicos regulada en el artículo 22 del Reglamento (UE) 910/2014.

Por lo que respecta a los certificados electrónicos, se introducen en la Ley varias disposiciones relativas a la expedición y contenido de los certificados cualificados, cuyo tiempo máximo de vigencia se mantiene en cinco años. En este sentido, no se permite a los prestadores de servicios el denominado «encadenamiento» en la renovación de certificados cualificados utilizando uno vigente, más que una sola vez, por razones de seguridad en el tráfico jurídico. Sin perjuicio de lo anterior, el Reglamento (UE) 910/2014 contempla la posibilidad de verificación de la identidad del solicitante de un certificado cualificado utilizando otros métodos de identificación reconocidos a escala nacional que garanticen una seguridad equivalente en términos de fiabilidad a la presencia física. Haciéndose eco de esta previsión, la Ley habilita a que reglamentariamente se regulen las condiciones y requisitos técnicos que lo harían posible.

Los certificados cualificados expedidos a personas físicas incluirán el número de Documento Nacional de Identidad, número de identidad de extranjero o número de identificación fiscal, salvo en los casos en los que el titular carezca de todos ellos. La misma regla se aplica en cuanto al número de identificación fiscal de las personas jurídicas o sin personalidad jurídica titulares de certificados cualificados, que en defecto de este han de utilizar un código que les identifique de forma unívoca y permanente en el tiempo, tal como se recoja en los registros oficiales.

En lo que se refiere a las obligaciones de los prestadores, la Ley establece el requisito de constitución de una garantía económica para la prestación de servicios cualificados de confianza. Se fija una cuantía mínima única de 1.500.000 euros, que se incrementa en 500.000 euros por cada tipo de servicio adicional que se preste, lo que se estima suficiente para cubrir los riesgos derivados del servicio, tiene en cuenta la diversidad de servicios en el mercado y no penaliza a los prestadores con mayor oferta.

Una de las exigencias del Reglamento (UE) 910/2014 se centra en garantizar la seguridad de los servicios de confianza frente a actos deliberados o fortuitos que afecten a sus productos, redes o sistemas de información. En este sentido, todos los prestadores de servicios de confianza, cualificados y no cualificados, están sometidos a la obligación de adoptar las medidas técnicas y organizativas adecuadas para gestionar los riesgos para la seguridad de los servicios de confianza que prestan, así como de notificar al órgano de supervisión cualquier violación de la seguridad o pérdida de la integridad que tenga un impacto significativo en el servicio de confianza prestado. Esta Ley sanciona el incumplimiento de las citadas obligaciones.

En respuesta a la evolución de la tecnología y las demandas del mercado, el Reglamento (UE) 910/2014 abre la posibilidad de prestación de servicios innovadores basados en soluciones móviles y en la nube, como la firma y sello electrónicos remotos, en los que el entorno es gestionado por un prestador de servicios de confianza en nombre del titular. A fin de garantizar que estos servicios electrónicos obtengan el mismo reconocimiento jurídico que aquellos utilizados en un entorno completamente gestionado por el usuario, estos prestadores deben aplicar procedimientos de seguridad específicos y utilizar sistemas y productos fiables, incluidos canales de comunicación electrónica seguros, para garantizar que el entorno es fiable y se utiliza bajo el control exclusivo del titular. Se pretende alcanzar, así, un equilibrio entre la facilidad para el acceso y el uso de los servicios, sin detrimento de la seguridad.

IV

Esta Ley deroga la Ley 59/2003, de 19 de diciembre, de firma electrónica, y con ella aquellos preceptos incompatibles con el Reglamento (UE) 910/2014.

Así sucede con los antiguos certificados de firma de personas jurídicas, introducidos por la citada Ley de firma electrónica. El nuevo paradigma instaurado por el mencionado

reglamento implica que únicamente las personas físicas están capacitadas para firmar electrónicamente, por lo que no prevé la emisión de certificados de firma electrónica a favor de personas jurídicas o entidades sin personalidad jurídica. A estas se reservan los sellos electrónicos, que permiten garantizar la autenticidad e integridad de documentos tales como facturas electrónicas. Sin perjuicio de lo anterior, las personas jurídicas podrán actuar por medio de los certificados de firma de aquellas personas físicas que legalmente les representen.

La Ley permite la posibilidad de que el órgano supervisor mantenga un servicio de difusión de información sobre los prestadores cualificados que operan en el mercado, con el fin de proporcionar a los usuarios información útil sobre los servicios que ofrecen en el desarrollo de su actividad.

Mediante la presente Ley se deroga también el artículo 25 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, referido a los terceros de confianza, debido a que los servicios ofrecidos por este tipo de proveedores se encuentran subsumidos en los tipos regulados por el Reglamento (UE) 910/2014, fundamentalmente en los servicios de entrega electrónica certificada y de conservación de firmas y sellos electrónicos.

V

Si bien la prestación de servicios electrónicos de confianza se realiza en régimen de libre competencia, el Reglamento (UE) 910/2014 prevé, para los servicios cualificados, un sistema de verificación previa de cumplimiento de los requisitos que en él se imponen. Así, se diseña un sistema mixto de colaboración público-privada para la supervisión de los prestadores cualificados, pues su inclusión en la lista de confianza, que permite iniciar esa actividad, debe basarse en un informe de evaluación de la conformidad emitido por un organismo de evaluación acreditado por un organismo nacional de acreditación, establecido en alguno de los Estados miembros de la Unión Europea. A partir de entonces, los prestadores cualificados deberán remitir el citado informe al menos cada veinticuatro meses.

Por su parte, los prestadores de servicios no cualificados pueden prestar servicios sin verificación previa de cumplimiento de requisitos, sin perjuicio de su sujeción a las potestades de seguimiento y control posterior de la Administración. No obstante, deberán comunicar al órgano supervisor la prestación del servicio en el plazo de tres meses desde que inicien su actividad, a los meros efectos de conocer su existencia y posibilitar su supervisión.

Por último, se define el régimen sancionador aplicable a los prestadores cualificados y no cualificados de servicios electrónicos de confianza, sin perjuicio de la posibilidad ya prevista en el artículo 20.3 del Reglamento (UE) 910/2014 de retirar la cualificación al prestador o servicio que presta, y su exclusión de la lista de confianza, en determinados supuestos. Asimismo, se han adecuado las cuantías de las sanciones, reduciéndose a la mitad la máxima imponible respecto a la legislación anterior, y se ha previsto la división en tramos de la horquilla sancionadora para la determinación de la multa imponible, en atención a los criterios de graduación concurrentes.

VI

Con arreglo a todo lo anterior, la presente Ley contiene veinte artículos, cuatro disposiciones adicionales, dos transitorias, una disposición derogatoria y siete disposiciones finales.

Las disposiciones adicionales se refieren: la primera a Fe pública y servicios electrónicos de confianza; la segunda a los efectos jurídicos de los sistemas utilizados en las Administraciones públicas; la tercera al Documento Nacional de Identidad y sus certificados electrónicos, y la cuarta al secreto de la identidad de los miembros del Centro Nacional de Inteligencia.

La disposición transitoria primera se refiere a la comunicación de actividad por prestadores de servicios no cualificados ya existentes, y la disposición transitoria segunda mantiene en vigor el Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del Documento Nacional de Identidad y sus certificados de firma electrónica, el

cual constituye desarrollo reglamentario parcial de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

En las disposiciones finales se modifican diversas leyes. En la primera, la Ley 56/2007, de 28 de diciembre, de medidas de impulso de la sociedad de la información, de forma que las empresas que presten servicios al público en general de especial trascendencia económica deberán disponer de un medio seguro de interlocución telemática, no necesariamente basado en certificados electrónicos. Con ello, se flexibiliza la norma y se da cabida a otros medios de identificación generalmente usados en el sector privado.

En la disposición final segunda, se modifica la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, con objeto de adaptarla al nuevo marco regulatorio de los servicios electrónicos de confianza definido en esta Ley y en el Reglamento (UE) 910/2014.

En la disposición final tercera, se modifica la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, para adaptar su regulación al Reglamento (UE) 2019/1150 del Parlamento Europeo y del Consejo, referente a plataformas digitales.

En la disposición final cuarta se introduce una nueva disposición adicional séptima en la Ley 17/2009, de 23 de noviembre, sobre el libre acceso a las actividades de servicios y su ejercicio, para adaptar su regulación al Reglamento (UE) 2018/302 del Parlamento Europeo y del Consejo, sobre medidas destinadas a impedir el bloqueo geográfico injustificado y otras formas de discriminación por razón de la nacionalidad, del lugar de residencia o del lugar de establecimientos de los clientes en el mercado interior.

La disposición final quinta contiene el título competencial, en virtud del cual la Ley se dicta al amparo de las competencias exclusivas que corresponden al Estado en materia de legislación civil, telecomunicaciones y seguridad pública, conforme al artículo 149.1.8.ª, 21.ª y 29.ª de la Constitución Española. El artículo 3 y la disposición final segunda se dictan, además, al amparo de lo previsto en el artículo 149.1.6.ª de la Constitución, el cual atribuye al Estado competencia exclusiva en materia de legislación procesal. Por su parte la disposición adicional segunda se dicta al amparo de lo previsto en el artículo 149.1.18.ª de la Constitución, en relación con la competencia estatal exclusiva sobre las bases del régimen jurídico de las Administraciones públicas y el procedimiento administrativo común.

Finalmente las disposiciones finales sexta y séptima se refieren al desarrollo reglamentario de la Ley y a su entrada en vigor, respectivamente.

TÍTULO I

Disposiciones generales

Artículo 1. *Objeto de la Ley.*

La presente Ley tiene por objeto regular determinados aspectos de los servicios electrónicos de confianza, como complemento del Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.

Artículo 2. *Ámbito de aplicación.*

Esta Ley se aplicará a los prestadores públicos y privados de servicios electrónicos de confianza establecidos en España.

Así mismo, se aplicará a los prestadores residentes o domiciliados en otro Estado que tengan un establecimiento permanente situado en España, siempre que ofrezcan servicios no supervisados por la autoridad competente de otro país de la Unión Europea.

Artículo 3. *Efectos jurídicos de los documentos electrónicos.*

1. Los documentos electrónicos públicos, administrativos y privados, tienen el valor y la eficacia jurídica que corresponda a su respectiva naturaleza, de conformidad con la legislación que les resulte aplicable.

2. La prueba de los documentos electrónicos privados en los que se hubiese utilizado un servicio de confianza no cualificado se regirá por lo dispuesto en el apartado 3 del artículo 326 de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil. Si el servicio fuese cualificado, se estará a lo previsto en el apartado 4 del mismo precepto.

TÍTULO II

Certificados electrónicos

Artículo 4. *Vigencia y caducidad de los certificados electrónicos.*

1. Los certificados electrónicos se extinguen por caducidad a la expiración de su período de vigencia, o mediante revocación por los prestadores de servicios electrónicos de confianza en los supuestos previstos en el artículo siguiente.

2. El período de vigencia de los certificados cualificados no será superior a cinco años.

Dicho período se fijará en atención a las características y tecnología empleada para generar los datos de creación de firma, sello, o autenticación de sitio web.

Artículo 5. *Revocación y suspensión de los certificados electrónicos.*

1. Los prestadores de servicios electrónicos de confianza extinguirán la vigencia de los certificados electrónicos mediante revocación en los siguientes supuestos:

a) Solicitud formulada por el firmante, la persona física o jurídica representada por este, un tercero autorizado, el creador del sello o el titular del certificado de autenticación de sitio web.

b) Violación o puesta en peligro del secreto de los datos de creación de firma o de sello, o del prestador de servicios de confianza, o de autenticación de sitio web, o utilización indebida de dichos datos por un tercero.

c) Resolución judicial o administrativa que lo ordene.

d) Fallecimiento del firmante; capacidad modificada judicialmente sobrevenida, total o parcial, del firmante; extinción de la personalidad jurídica o disolución del creador del sello en el caso de tratarse de una entidad sin personalidad jurídica, y cambio o pérdida de control sobre el nombre de dominio en el supuesto de un certificado de autenticación de sitio web.

e) Terminación de la representación en los certificados electrónicos con atributo de representante. En este caso, tanto el representante como la persona o entidad representada están obligados a solicitar la revocación de la vigencia del certificado en cuanto se produzca la modificación o extinción de la citada relación de representación.

f) Cese en la actividad del prestador de servicios de confianza salvo que la gestión de los certificados electrónicos expedidos por aquel sea transferida a otro prestador de servicios de confianza.

g) Descubrimiento de la falsedad o inexactitud de los datos aportados para la expedición del certificado y que consten en él, o alteración posterior de las circunstancias verificadas para la expedición del certificado, como las relativas al cargo.

h) En caso de que se advierta que los mecanismos criptográficos utilizados para la generación de los certificados no cumplen los estándares de seguridad mínimos necesarios para garantizar su seguridad.

i) Cualquier otra causa lícita prevista en la declaración de prácticas del servicio de confianza.

2. Los prestadores de servicios de confianza suspenderán la vigencia de los certificados electrónicos en los supuestos previstos en las letras a), c) y h) del apartado anterior, así como en los casos de duda sobre la concurrencia de las circunstancias previstas en sus letras b) y g), siempre que sus declaraciones de prácticas de certificación prevean la posibilidad de suspender los certificados.

3. En su caso, y de manera previa o simultánea a la indicación de la revocación o suspensión de un certificado electrónico en el servicio de consulta sobre el estado de validez o revocación de los certificados por él expedidos, el prestador de servicios electrónicos de confianza comunicará al titular, por un medio que acredite la entrega y recepción efectiva

siempre que sea factible, esta circunstancia, especificando los motivos y la fecha y la hora en que el certificado quedará sin efecto.

En los casos de suspensión, la vigencia del certificado se extinguirá si transcurrido el plazo de duración de la suspensión, el prestador no la hubiera levantado.

Artículo 6. *Identidad y atributos de los titulares de certificados cualificados.*

1. La identidad del titular en los certificados cualificados se consignará de la siguiente forma:

a) En el supuesto de certificados de firma electrónica y de autenticación de sitio web expedidos a personas físicas, por su nombre y apellidos y su número de Documento Nacional de Identidad, número de identidad de extranjero o número de identificación fiscal, o a través de un pseudónimo que conste como tal de manera inequívoca. Los números anteriores podrán sustituirse por otro código o número identificativo únicamente en caso de que el titular carezca de todos ellos por causa lícita, siempre que le identifique de forma unívoca y permanente en el tiempo.

b) En el supuesto de certificados de sello electrónico y de autenticación de sitio web expedidos a personas jurídicas, por su denominación o razón social y su número de identificación fiscal. En defecto de este, deberá indicarse otro código identificativo que le identifique de forma unívoca y permanente en el tiempo, tal como se recoja en los registros oficiales.

2. Si los certificados admiten una relación de representación incluirán la identidad de la persona física o jurídica representada en las formas previstas en el apartado anterior, así como una indicación del documento, público si resulta exigible, que acredite de forma fehaciente las facultades del firmante para actuar en nombre de la persona o entidad a la que represente y, en caso de ser obligatoria la inscripción, de los datos registrales.

Artículo 7. *Comprobación de la identidad y otras circunstancias de los solicitantes de un certificado cualificado.*

1. La identificación de la persona física que solicite un certificado cualificado exigirá su personación ante los encargados de verificarla y se acreditará mediante el Documento Nacional de Identidad, pasaporte u otros medios admitidos en Derecho. Podrá prescindirse de la personación de la persona física que solicite un certificado cualificado si su firma en la solicitud de expedición de un certificado cualificado ha sido legitimada en presencia notarial.

2. Reglamentariamente, mediante Orden de la persona titular del Ministerio de Asuntos Económicos y Transformación Digital, se determinarán otras condiciones y requisitos técnicos de verificación de la identidad a distancia y, si procede, otros atributos específicos de la persona solicitante de un certificado cualificado, mediante otros métodos de identificación como videoconferencia o vídeo-identificación que aporten una seguridad equivalente en términos de fiabilidad a la presencia física según su evaluación por un organismo de evaluación de la conformidad. La determinación de dichas condiciones y requisitos técnicos se realizará a partir de los estándares que, en su caso, hayan sido determinados a nivel comunitario.

Serán considerados métodos de identificación reconocidos a escala nacional, a los efectos de lo previsto en el presente apartado, aquellos que aporten una seguridad equivalente en términos de fiabilidad a la presencia física y cuya equivalencia en el nivel de seguridad sea certificada por un organismo de evaluación de la conformidad, de acuerdo con lo previsto en la normativa en materia de servicios electrónicos de confianza.

3. La forma en que se ha procedido a identificar a la persona física solicitante podrá constar en el certificado. En otro caso, los prestadores de servicios de confianza deberán colaborar entre sí para determinar cuándo se produjo la última personación.

4. En el caso de certificados cualificados de sello electrónico y de firma electrónica con atributo de representante, los prestadores de servicios de confianza comprobarán, además de los datos señalados en los apartados anteriores, los datos relativos a la constitución y personalidad jurídica, y a la persona o entidad representada, respectivamente, así como la extensión y vigencia de las facultades de representación del solicitante mediante los documentos, públicos si resultan exigibles, que sirvan para acreditar los extremos citados de

manera fehaciente y su inscripción en el correspondiente registro público si así resulta exigible. Esta comprobación podrá realizarse, asimismo, mediante consulta en el registro público en el que estén inscritos los documentos de constitución y de apoderamiento, pudiendo emplear los medios telemáticos facilitados por los citados registros públicos.

5. Cuando el certificado cualificado contenga otras circunstancias personales o atributos del solicitante, como su condición de titular de un cargo público, su pertenencia a un colegio profesional o su titulación, estas deberán comprobarse mediante los documentos oficiales que las acrediten, de conformidad con su normativa específica.

6. Lo dispuesto en los apartados anteriores podrá no ser exigible cuando la identidad u otras circunstancias permanentes de los solicitantes de los certificados constaran ya al prestador de servicios de confianza en virtud de una relación preexistente, en la que, para la identificación del interesado, se hubiese empleado el medio señalado en el apartado 1 y el período de tiempo transcurrido desde la identificación fuese menor de cinco años.

7. El Ministerio de Asuntos Económicos y Transformación Digital velará por que los prestadores cualificados de servicios electrónicos de confianza puedan contribuir a la elaboración de la norma reglamentaria prevista en el apartado 2 del presente artículo, de acuerdo con lo previsto en el artículo 26.6 de la Ley 50/1997, de 27 de noviembre, del Gobierno.

TÍTULO III

Obligaciones y responsabilidad de los prestadores de servicios electrónicos de confianza

Artículo 8. *Protección de los datos personales.*

1. El tratamiento de los datos personales que precisen los prestadores de servicios electrónicos de confianza para el desarrollo de su actividad y los órganos administrativos para el ejercicio de las funciones atribuidas por esta Ley se sujetará a lo dispuesto en la legislación aplicable en materia de protección de datos de carácter personal.

2. Los prestadores de servicios electrónicos de confianza que consignen un pseudónimo en un certificado electrónico deberán constatar la verdadera identidad del titular del certificado y conservar la documentación que la acredite.

3. Dichos prestadores de servicios de confianza estarán obligados a revelar la citada identidad cuando lo soliciten los órganos judiciales y otras autoridades públicas en el ejercicio de funciones legalmente atribuidas, con sujeción a lo dispuesto en la legislación aplicable en materia de protección de datos personales.

Artículo 9. *Obligaciones de los prestadores de servicios electrónicos de confianza.*

1. Los prestadores de servicios electrónicos de confianza deberán:

a) Publicar información veraz y acorde con esta Ley y el Reglamento (UE) 910/2014.

b) No almacenar ni copiar, por sí o a través de un tercero, los datos de creación de firma, sello o autenticación de sitio web de la persona física o jurídica a la que hayan prestado sus servicios, salvo en caso de su gestión en nombre del titular.

En este caso, utilizarán sistemas y productos fiables, incluidos canales de comunicación electrónica seguros, y se aplicarán procedimientos y mecanismos técnicos y organizativos adecuados, para garantizar que el entorno sea fiable y se utilice bajo el control exclusivo del titular del certificado. Además, deberán custodiar y proteger los datos de creación de firma, sello o autenticación de sitio web frente a cualquier alteración, destrucción o acceso no autorizado, así como garantizar su continua disponibilidad.

2. Los prestadores de servicios de confianza que expidan certificados electrónicos deberán disponer de un servicio de consulta sobre el estado de validez o revocación de los certificados emitidos accesible al público.

3. Los prestadores cualificados de servicios electrónicos de confianza deberán cumplir las siguientes obligaciones adicionales:

a) El período de tiempo durante el que deberán conservar la información relativa a los servicios prestados de acuerdo con el artículo 24.2.h) del Reglamento (UE) 910/2014, será de 15 años desde la extinción del certificado o la finalización del servicio prestado.

En caso de que expidan certificados cualificados de sello electrónico o autenticación de sitio web a personas jurídicas, los prestadores de servicios de confianza registrarán también la información que permita determinar la identidad de la persona física a la que se hayan entregado los citados certificados, para su identificación en procedimientos judiciales o administrativos.

b) Constituir un seguro de responsabilidad civil por importe mínimo de 1.500.000 euros, excepto si el prestador pertenece al sector público. Si presta más de un servicio cualificado de los previstos en el Reglamento (UE) 910/2014, se añadirán 500.000 euros más por cada tipo de servicio.

La citada garantía podrá ser sustituida total o parcialmente por una garantía mediante aval bancario o seguro de caución, de manera que la suma de las cantidades aseguradas sea coherente con lo dispuesto en el párrafo anterior.

Las cuantías y los medios de aseguramiento y garantía establecidos en los dos párrafos anteriores podrán ser modificados mediante real decreto.

c) El prestador cualificado que vaya a cesar en su actividad deberá comunicarlo a los clientes a los que preste sus servicios y al órgano de supervisión con una antelación mínima de dos meses al cese efectivo de la actividad, por un medio que acredite la entrega y recepción efectiva siempre que sea factible. El plan de cese del prestador de servicios puede incluir la transferencia de clientes, una vez acreditada la ausencia de oposición de los mismos, a otro prestador cualificado, el cual podrá conservar la información relativa a los servicios prestados hasta entonces.

Igualmente, comunicará al órgano de supervisión cualquier otra circunstancia relevante que pueda impedir la continuación de su actividad. En especial, deberá comunicar, en cuanto tenga conocimiento de ello, la apertura de cualquier proceso concursal que se siga contra él.

d) Enviar el informe de evaluación de la conformidad al Ministerio de Asuntos Económicos y Transformación Digital en los términos previstos en el artículo 20.1 del Reglamento (UE) 910/2014. El incumplimiento de esta obligación conllevará la retirada de la cualificación al prestador y al servicio que este presta, y su eliminación de la lista de confianza prevista en el artículo 22 del citado Reglamento, previo requerimiento al prestador del servicio para que cese en el citado incumplimiento.

Artículo 10. *Responsabilidad de los prestadores de servicios electrónicos de confianza.*

Los prestadores de servicios electrónicos de confianza asumirán toda la responsabilidad frente a terceros por la actuación de las personas u otros prestadores en los que deleguen la ejecución de alguna o algunas de las funciones necesarias para la prestación de servicios electrónicos de confianza, incluyendo las actuaciones de comprobación de identidad previas a la expedición de un certificado cualificado.

Artículo 11. *Limitaciones de responsabilidad de los prestadores de servicios electrónicos de confianza.*

1. El prestador de servicios electrónicos de confianza no será responsable de los daños y perjuicios ocasionados a la persona a la que ha prestado sus servicios o a terceros de buena fe, si esta incurre en alguno de los supuestos previstos en el Reglamento (UE) 910/2014 o en los siguientes:

a) No haber proporcionado al prestador de servicios de confianza información veraz, completa y exacta para la prestación del servicio de confianza, en particular, sobre los datos que deban constar en el certificado electrónico o que sean necesarios para su expedición o para la extinción o suspensión de su vigencia, cuando su inexactitud no haya podido ser detectada, actuando con la debida diligencia, por el prestador de servicios.

b) La falta de comunicación sin demora indebida al prestador de servicios de cualquier modificación de las circunstancias que incidan en la prestación del servicio de confianza, en particular, aquellas reflejadas en el certificado electrónico.

c) Negligencia en la conservación de sus datos de creación de firma, sello o autenticación de sitio web, en el aseguramiento de su confidencialidad y en la protección de todo acceso o revelación de estos o, en su caso, de los medios que den acceso a ellos.

d) No solicitar la suspensión o revocación del certificado electrónico en caso de duda en cuanto al mantenimiento de la confidencialidad de sus datos de creación de firma, sello o autenticación de sitio web o, en su caso, de los medios que den acceso a ellos.

e) Utilizar los datos de creación de firma, sello o autenticación de sitio web cuando haya expirado el período de validez del certificado electrónico o el prestador de servicios de confianza le notifique la extinción o suspensión de su vigencia.

2. El prestador de servicios de confianza tampoco será responsable por los daños y perjuicios si el destinatario actúa de forma negligente. Se entenderá que el destinatario actúa de forma negligente cuando no tenga en cuenta la suspensión o pérdida de vigencia del certificado electrónico, o cuando no verifique la firma o sello electrónico.

3. El prestador de servicios de confianza no será responsable por los daños y perjuicios en caso de inexactitud de los datos que consten en el certificado electrónico si estos le han sido acreditados mediante documento público u oficial, inscrito en un registro público si así resulta exigible.

Artículo 12. *Inicio de la prestación de servicios electrónicos de confianza no cualificados.*

Los prestadores de servicios de confianza no cualificados no necesitan verificación administrativa previa de cumplimiento de requisitos para iniciar su actividad, pero deberán comunicar su actividad al Ministerio de Asuntos Económicos y Transformación Digital en el plazo de tres meses desde que la inicien, que publicará en su página web el listado de prestadores de servicios de confianza no cualificados en una lista diferente a la de los prestadores de servicios de confianza cualificados, con la descripción detallada y clara de las características propias y diferenciales de los prestadores cualificados y de los prestadores no cualificados.

En el mismo plazo deberán comunicar la modificación de los datos inicialmente transmitidos y el cese de su actividad.

Artículo 13. *Obligaciones de seguridad de la información.*

1. Los prestadores cualificados y no cualificados de servicios electrónicos de confianza notificarán al Ministerio de Asuntos Económicos y Transformación Digital las violaciones de seguridad o pérdidas de la integridad señaladas en el artículo 19.2 del Reglamento (UE) 910/2014, sin perjuicio de su notificación a la Agencia Española de Protección de Datos, a otros organismos relevantes o a las personas afectadas.

2. Los prestadores de servicios tienen la obligación de tomar las medidas necesarias para resolver los incidentes de seguridad que les afecten.

3. Los prestadores de servicios ampliarán, en un plazo máximo de un mes tras la notificación del incidente y, de haber tenido lugar, tras su resolución, la información suministrada en la notificación inicial con arreglo a las directrices y formularios que pueda establecer el Ministerio de Asuntos Económicos y Transformación Digital.

TÍTULO IV

Supervisión y control

Artículo 14. *Órgano de supervisión.*

1. El Ministerio de Asuntos Económicos y Transformación Digital, como órgano de supervisión, controlará el cumplimiento por los prestadores de servicios electrónicos de confianza cualificados y no cualificados que ofrezcan sus servicios al público de las obligaciones establecidas en el Reglamento (UE) 910/2014 y en esta Ley.

2. El Ministerio de Asuntos Económicos y Transformación Digital podrá acordar las medidas apropiadas para el cumplimiento del Reglamento (UE) 910/2014 y de esta Ley.

En particular, podrá dictar directrices para la elaboración y comunicación de informes y documentos, así como recomendaciones para el cumplimiento de las obligaciones técnicas y de seguridad exigibles a los servicios de confianza, así como sobre requisitos y normas técnicas de auditoría y certificación para la evaluación de la conformidad de los prestadores cualificados de servicios de confianza. Al efecto, se tendrán en consideración las normas, instrucciones, guías y recomendaciones emitidas por el Centro Criptológico Nacional en el marco de sus competencias, así como informes, especificaciones o normas elaboradas por la Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA) o por organismos de estandarización europeos e internacionales.

Artículo 15. *Actuaciones inspectoras.*

1. El Ministerio de Asuntos Económicos y Transformación Digital realizará las actuaciones inspectoras que sean precisas para el ejercicio de su función de supervisión y control. Los funcionarios adscritos al Ministerio de Asuntos Económicos y Transformación Digital que realicen la inspección tendrán la consideración de autoridad pública en el desempeño de sus cometidos.

2. El Ministerio de Asuntos Económicos y Transformación Digital podrá recurrir a entidades independientes y técnicamente cualificadas para que le asistan en las labores de supervisión y control sobre los prestadores de servicios de confianza que le asigna el Reglamento (UE) 910/2014 y esta Ley.

3. Podrá requerirse la realización de pruebas en laboratorios o entidades especializadas para acreditar el cumplimiento de determinados requisitos. En este caso, los prestadores de servicios correrán con los gastos que ocasione esta evaluación.

Artículo 16. *Mantenimiento de la lista de confianza.*

1. El Ministerio de Asuntos Económicos y Transformación Digital establecerá, mantendrá y publicará la lista de confianza con información relativa a los prestadores cualificados de servicios de confianza sujetos a esta Ley, junto con la información relacionada con los servicios de confianza cualificados prestados por ellos, según lo previsto en el artículo 22 del Reglamento (UE) 910/2014.

2. El plazo máximo para dictar y notificar resolución en el procedimiento de verificación previa de cumplimiento de los requisitos establecidos en el citado Reglamento será de 6 meses, transcurridos los cuales se podrá entender desestimada la solicitud.

3. La revocación de la cualificación a un prestador o a un servicio mediante su retirada de la lista de confianza es independiente de la aplicación del régimen sancionador.

Artículo 17. *Información y colaboración.*

1. Los prestadores de servicios de confianza, la entidad nacional de acreditación, los organismos de evaluación de la conformidad, los organismos de certificación y cualquier otra persona o entidad relacionada con el prestador de servicios de confianza, tienen la obligación de facilitar al Ministerio de Asuntos Económicos y Transformación Digital toda la información y colaboración precisas para el ejercicio de sus funciones.

Si el organismo de certificación perteneciera a la Autoridad Nacional de Certificación de la Ciberseguridad o estuviese supervisado por ella, se acordarán con dicha Autoridad los mecanismos de colaboración y el contenido de la información necesaria.

Los prestadores de servicios de confianza deberán permitir a sus funcionarios o al personal inspector el acceso a sus instalaciones y la consulta de cualquier documentación relevante para la inspección de que se trate, siendo de aplicación, en su caso, lo dispuesto en el artículo 8.6 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa. En sus inspecciones podrán ir acompañados de expertos o peritos en las materias sobre las que versen aquellas.

2. La información referente a los prestadores cualificados de servicios de confianza podrá ser objeto de publicación en la dirección de Internet del Ministerio de Asuntos Económicos y Transformación Digital para su difusión y conocimiento.

3. A más tardar el 1 de febrero de cada año, los prestadores cualificados de servicios de confianza remitirán al Ministerio de Asuntos Económicos y Transformación Digital un informe

sobre sus datos de actividad del año civil precedente, con objeto de cumplimiento por parte de este de las obligaciones de información a la Comisión Europea.

4. El Ministerio de Asuntos Económicos y Transformación Digital informará a la Agencia Española de Protección de Datos en caso de resultar infringidas las normas sobre protección de datos de carácter personal, así como sobre los incidentes en materia de seguridad que impliquen violaciones de los datos de carácter personal.

TÍTULO V

Infracciones y sanciones

Artículo 18. *Infracciones.*

1. Las infracciones de los preceptos del Reglamento (UE) 910/2014 y de esta Ley se clasifican en muy graves, graves y leves.

2. Son infracciones muy graves:

a) La comisión de una infracción grave en el plazo de dos años desde que hubiese sido sancionado por una infracción grave de la misma naturaleza, contados desde que recaiga la resolución sancionadora firme.

b) La expedición de certificados cualificados sin realizar todas las comprobaciones previas relativas a la identidad u otras circunstancias del titular del certificado o al poder de representación de quien lo solicita en su nombre, señaladas en el Reglamento (UE) 910/2014 y en esta Ley, cuando ello afecte a la mayoría de los certificados cualificados expedidos en el año anterior al inicio del procedimiento sancionador o desde el inicio de la actividad del prestador si este periodo es menor.

3. Son infracciones graves:

a) La resistencia, obstrucción, excusa o negativa a la actuación inspectora de los órganos facultados para llevarla a cabo con arreglo a esta Ley.

b) Actuar en el mercado como prestador cualificado de servicios de confianza, ofrecer servicios de confianza como cualificados o utilizar la etiqueta de confianza «UE» sin haber obtenido la cualificación de los citados servicios.

c) En caso de que el prestador expida certificados electrónicos, almacenar o copiar, por sí o a través de un tercero, los datos de creación de firma, sello o autenticación de sitio web de la persona física o jurídica a la que hayan prestado sus servicios, salvo en caso de su gestión en nombre del titular.

d) No proteger adecuadamente los datos de creación de firma, sello o autenticación de sitio web cuya gestión se le haya encomendado en la forma establecida en el artículo 9.1.b) de esta Ley.

e) No registrar o conservar la información a la que se refiere el artículo 9.3.a) de esta Ley.

f) El incumplimiento de la obligación de notificación de incidentes establecida en el artículo 19.2 del Reglamento (UE) 910/2014, en los términos previstos en el artículo 13 de esta Ley.

g) En caso de prestadores cualificados de servicios de confianza, el incumplimiento de alguna de las obligaciones establecidas en los artículos 24.2, letras b), c), d), e), f), g), h), y k), 24.3 y 24.4 del Reglamento (UE) 910/2014, con las precisiones establecidas, en su caso, por esta Ley.

h) La expedición de certificados cualificados sin realizar todas las comprobaciones previas relativas a la identidad u otras circunstancias del titular del certificado o al poder de representación de quien lo solicita en su nombre, señaladas en el Reglamento (UE) 910/2014 y en esta Ley, cuando no constituya infracción muy grave.

i) La ausencia de adopción de medidas, o la adopción de medidas insuficientes, para la resolución de los incidentes de seguridad en los productos, redes y sistemas de información, en el plazo de diez días desde que aquellos se hubieren producido.

j) El incumplimiento de las resoluciones dictadas por el Ministerio de Asuntos Económicos y Transformación Digital para requerir a un prestador de servicios de confianza

que corrija cualquier incumplimiento de los requisitos establecidos en esta Ley y en el Reglamento (UE) 910/2014.

k) La falta o deficiente presentación de información solicitada por parte del Ministerio de Asuntos Económicos y Transformación Digital en su función de inspección y control, a partir del segundo requerimiento.

l) No cumplir con las obligaciones de constatar la verdadera identidad del titular de un certificado electrónico y de conservar la documentación que la acredite, en caso de consignación de un pseudónimo.

m) El incumplimiento por parte de los prestadores cualificados y no cualificados de servicios de confianza de la obligación establecida en el artículo 19.1 del Reglamento (UE) 910/2014 de adoptar las medidas técnicas y organizativas adecuadas para gestionar los riesgos para la seguridad de los servicios de confianza que presten.

n) No extinguir la vigencia de los certificados electrónicos en los supuestos señalados en esta Ley.

o) La prestación de servicios cualificados careciendo del correspondiente seguro obligatorio, en los términos previstos en el artículo 9.3.b) de esta Ley.

4. Constituyen infracciones leves:

a) Publicar información no veraz o no acorde con esta Ley y el Reglamento (UE) 910/2014.

b) No comunicar el inicio de actividad, su modificación o cese por los prestadores de servicios no cualificados en el plazo establecido en el artículo 12 de esta Ley.

c) El incumplimiento por los prestadores cualificados de servicios de confianza de alguna de las obligaciones establecidas en el artículo 24.2, letras a) e i) del Reglamento (UE) 910/2014.

d) El incumplimiento por los prestadores cualificados de servicios de confianza de su obligación de remitir un informe anual de actividad al Ministerio de Asuntos Económicos y Transformación Digital antes del 1 de febrero de cada año.

e) El incumplimiento del deber de comunicación establecido en el artículo 9.3.c) de esta Ley.

f) La falta o deficiente presentación de información solicitada por parte del Ministerio de Asuntos Económicos y Transformación Digital en su función de inspección y control.

Artículo 19. *Sanciones.*

1. Por la comisión de infracciones recogidas en el artículo anterior, se impondrán al infractor las siguientes sanciones:

a) Por la comisión de infracciones muy graves, una multa por importe de 150.001 hasta 300.000 euros.

b) Por la comisión de infracciones graves, una multa por importe de 50.001 hasta 150.000 euros.

c) Por la comisión de infracciones leves, una multa por importe de hasta 50.000 euros.

2. La cuantía de las sanciones que se impongan se determinará aplicando una graduación de importe mínimo, medio y máximo a cada nivel de infracción, teniendo en cuenta lo siguiente:

a) El grado de culpabilidad o la existencia de intencionalidad.

b) La continuidad o persistencia en la conducta infractora.

c) La naturaleza y cuantía de los perjuicios causados.

d) La reincidencia, por comisión en el término de un año de más de una infracción de la misma naturaleza cuando así haya sido declarado por resolución firme en vía administrativa.

e) El volumen de facturación del prestador responsable.

f) El número de personas afectadas por la infracción.

g) La gravedad del riesgo generado por la conducta.

h) Las acciones realizadas por el prestador encaminadas a paliar los efectos o consecuencias de la infracción.

3. Las resoluciones sancionadoras por la comisión de infracciones muy graves serán publicadas en el sitio de Internet del Ministerio de Asuntos Económicos y Transformación Digital, con indicación, en su caso, de los recursos interpuestos contra ellas.

Artículo 19 bis. *Apercibimiento.*

1. Los órganos con competencia sancionadora, atendida la naturaleza de los hechos y la concurrencia significativa de los criterios establecidos en el artículo anterior, podrán acordar no iniciar la apertura del procedimiento sancionador y, en su lugar, apercibir al sujeto responsable, a fin de que en el plazo que el órgano sancionador determine, acredite la adopción de las medidas correctoras que, en cada caso, resulten pertinentes, siempre que los hechos fuesen constitutivos de infracción leve o grave conforme a lo dispuesto en esta ley.

2. Si el apercibimiento no fuera atendido en el plazo que el órgano sancionador hubiera determinado, procederá la apertura del correspondiente procedimiento sancionador por dicho incumplimiento.

Artículo 20. *Potestad sancionadora.*

1. La imposición de sanciones por el incumplimiento de lo previsto en esta ley corresponderá, en el caso de infracciones muy graves, a la persona titular del Ministerio de Asuntos Económicos y Transformación Digital, y en el de infracciones graves y leves, a la persona titular de la Secretaría de Estado de Digitalización e Inteligencia Artificial.

2. La potestad sancionadora regulada en esta ley se ejercerá de conformidad con lo establecido al respecto en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y en sus normas de desarrollo. El procedimiento tendrá una duración máxima de nueve meses a contar desde la fecha del acuerdo de iniciación. El plazo máximo de duración del procedimiento simplificado será de tres meses.

Disposición adicional primera. *Fe pública y servicios electrónicos de confianza.*

Lo dispuesto en esta Ley no sustituye ni modifica las normas que regulan las funciones que corresponden a los funcionarios que tengan legalmente atribuida la facultad de dar fe en documentos en lo que se refiere al ámbito de sus competencias.

Disposición adicional segunda. *Efectos jurídicos de los sistemas utilizados en las Administraciones públicas.*

Todos los sistemas de identificación, firma y sello electrónico previstos en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, tendrán plenos efectos jurídicos.

Disposición adicional tercera. *Documento Nacional de Identidad y sus certificados electrónicos.*

1. El Documento Nacional de Identidad electrónico es el Documento Nacional de Identidad que permite acreditar electrónicamente la identidad personal de su titular, en los términos establecidos en el artículo 8 de la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana, así como la firma electrónica de documentos.

2. Todas las personas físicas o jurídicas, públicas o privadas, reconocerán la eficacia del Documento Nacional de Identidad para acreditar la identidad y los demás datos personales del titular que consten en el mismo, así como la identidad del firmante y la integridad de los documentos firmados con sus certificados electrónicos.

3. Los órganos competentes del Ministerio del Interior para la expedición del Documento Nacional de Identidad cumplirán las obligaciones que la presente Ley impone a los prestadores de servicios electrónicos de confianza que expidan certificados cualificados.

4. Sin perjuicio de la aplicación de la normativa vigente en materia del Documento Nacional de Identidad en todo aquello que se adecúe a sus características particulares, el Documento Nacional de Identidad se regirá por su normativa específica.

Disposición adicional cuarta. *Secreto de la identidad de los miembros del Centro Nacional de Inteligencia.*

Lo dispuesto en los artículos 7 y 8 de esta Ley se entenderá sin perjuicio de lo dispuesto en la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, en relación con la obligación de guardar secreto sobre la identidad de sus miembros.

Disposición transitoria primera. *Comunicación de actividad por prestadores de servicios no cualificados ya existentes.*

Los prestadores de servicios no cualificados que ya vinieran prestando servicios deberán comunicar su actividad al Ministerio de Asuntos Económicos y Transformación Digital en el plazo de tres meses a contar desde la entrada en vigor de esta Ley.

Se exceptúan aquellos que hubieran comunicado los servicios prestados al Ministerio de Asuntos Económicos y Transformación Digital antes de la entrada en vigor de esta Ley.

Disposición transitoria segunda. *Desarrollo reglamentario del Documento Nacional de Identidad.*

Hasta que se desarrolle reglamentariamente el Documento Nacional de Identidad, se mantendrá en vigor el Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del Documento Nacional de Identidad y sus certificados de firma electrónica.

Disposición derogatoria.

Quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en esta Ley, y en particular:

a) La Ley 59/2003, de 19 de diciembre, de firma electrónica.

b) El artículo 25 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

c) La Orden del Ministerio de Fomento de 21 de febrero de 2000 por la que se aprueba el Reglamento de acreditación de prestadores de servicios de certificación y de certificación de determinados productos de firma electrónica.

Disposición final primera. *Modificación de la Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.*

Se modifica el apartado 1 del artículo 2 de la Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información, que queda redactado como sigue:

> «1. Sin perjuicio de la utilización de otros medios de comunicación a distancia con los clientes, las empresas que presten servicios al público en general de especial trascendencia económica deberán facilitar a sus usuarios un medio seguro de interlocución telemática que les permita la realización de, al menos, los siguientes trámites:
>
> a) Contratación electrónica de servicios, suministros y bienes, la modificación y finalización o rescisión de los correspondientes contratos, así como cualquier acto o negocio jurídico entre las partes, sin perjuicio de lo establecido en la normativa sectorial.
>
> b) Consulta de sus datos de cliente, que incluirán información sobre su historial de facturación de, al menos, los últimos tres años y el contrato suscrito, incluidas las condiciones generales si las hubiere.
>
> c) Presentación de quejas, incidencias, sugerencias y, en su caso, reclamaciones, garantizando la constancia de su presentación para el consumidor y asegurando una atención personal directa.
>
> d) Ejercicio de sus derechos de acceso, rectificación, cancelación y oposición en los términos previstos en la normativa reguladora de protección de datos de carácter personal.»

Disposición final segunda. *Modificación de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.*

Uno. Se modifica el apartado 3 del artículo 326 de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, que queda redactado en los siguientes términos:

«3. Cuando la parte a quien interese la eficacia de un documento electrónico lo solicite o se impugne su autenticidad, integridad, precisión de fecha y hora u otras características del documento electrónico que un servicio electrónico de confianza no cualificado de los previstos en el Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, permita acreditar, se procederá con arreglo a lo establecido en el apartado 2 del presente artículo y en el Reglamento (UE) n.º 910/2014.»

Dos. Se añade un apartado 4 al citado artículo 326, con el siguiente tenor:

«4. Si se hubiera utilizado algún servicio de confianza cualificado de los previstos en el Reglamento citado en el apartado anterior, se presumirá que el documento reúne la característica cuestionada y que el servicio de confianza se ha prestado correctamente si figuraba, en el momento relevante a los efectos de la discrepancia, en la lista de confianza de prestadores y servicios cualificados.

Si aun así se impugnare el documento electrónico, la carga de realizar la comprobación corresponderá a quien haya presentado la impugnación. Si dichas comprobaciones obtienen un resultado negativo, serán las costas, gastos y derechos que origine la comprobación exclusivamente a cargo de quien hubiese formulado la impugnación. Si, a juicio del tribunal, la impugnación hubiese sido temeraria, podrá imponerle, además, una multa de 300 a 1200 euros.»

Disposición final tercera. *Modificación de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.*

La Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, se modifica en los siguientes términos:

Uno. Se añade un nuevo artículo 12 ter que queda redactado como sigue:

«Artículo 12 ter. *Obligaciones relativas a la portabilidad de datos no personales.*

Los proveedores de servicios de intermediación que alojen o almacenen datos de usuarios a los que presten servicios de redes sociales o servicios de la sociedad de la información equivalentes deberán remitir a dichos usuarios, a su solicitud, los contenidos que les hubieran facilitado, sin impedir su transmisión posterior a otro proveedor. La remisión deberá efectuarse en un formato estructurado, de uso común y lectura mecánica.

Asimismo, deberán transmitir dichos contenidos directamente a otro proveedor designado por el usuario, siempre que sea técnicamente posible, según prevé el artículo 95 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.

Para el cumplimiento de estas obligaciones será aplicable lo dispuesto en el artículo 12.5 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.»

Dos. El primer párrafo del apartado 1 del artículo 35 queda redactado como sigue:

«1. El Ministerio de Asuntos Económicos y Transformación Digital controlará el cumplimiento por los prestadores de servicios de la sociedad de la información de las obligaciones establecidas en esta Ley y en sus disposiciones de desarrollo, en lo que se refiere a los servicios propios de la sociedad de la información, así como en el Reglamento (UE) 2019/1150 del Parlamento Europeo y del Consejo, de 20 de junio de

2019, sobre el fomento de la equidad y la transparencia para los usuarios profesionales de servicios de intermediación en línea, por parte de aquellos proveedores incluidos en su ámbito de aplicación.»

Tres. Se añade un nuevo artículo 36 bis que queda redactado como sigue:

«Artículo 36 bis. *Deber de comunicación de las organizaciones y asociaciones representativas de usuarios profesionales o de los usuarios de sitios web corporativos.*

Las organizaciones y asociaciones que posean un interés legítimo de representación de usuarios profesionales o de los usuarios de sitios web corporativos, y que, cumpliendo con los requisitos del artículo 14.3 del Reglamento (UE) 2019/1150, hubieren solicitado al Ministerio de Asuntos Económicos y Transformación Digital su inclusión en la lista elaborada al efecto por la Comisión Europea, notificarán inmediatamente al citado Ministerio cualquier circunstancia que afecte a su entidad que derive en un incumplimiento sobrevenido de los mencionados requisitos.»

Cuatro. El primer párrafo del artículo 37 queda redactado como sigue:

«Los prestadores de servicios de la sociedad de la información a los que les sea de aplicación la presente Ley, así como los proveedores incluidos en el ámbito de aplicación del Reglamento (UE) 2019/1150, están sujetos al régimen sancionador establecido en este Título.»

Cinco. Se añaden doce nuevas letras de la j) a la u) al apartado 3 del artículo 38 con la siguiente redacción:

«j) La exigencia del pago de un canon por atender la obligación prevista en el artículo 12 ter, fuera de los supuestos establecidos en el artículo 12.5 del Reglamento (UE) 2016/679.

k) El incumplimiento habitual de la obligación prevista en el artículo 12 ter.

l) El incumplimiento habitual por parte de los proveedores de servicios de intermediación en línea de la obligación establecida en el apartado 5 del artículo 3 del Reglamento (UE) 2019/1150 en materia de visibilidad de la identidad del usuario profesional.

m) El incumplimiento habitual por parte de los proveedores de servicios de intermediación en línea de cualquiera de las obligaciones en materia de restricción, suspensión y terminación del servicio establecidas en los apartados 1, 2 y 3 del artículo 4 del Reglamento (UE) 2019/1150.

n) El incumplimiento habitual por parte de los proveedores de servicios de intermediación en línea o proveedores de motores de búsqueda en línea de cualquiera de las obligaciones en materia de clasificación establecidas en el artículo 5 del Reglamento (UE) 2019/1150 que les resulten aplicables.

o) El incumplimiento habitual por parte de los proveedores de servicios de intermediación en línea de la obligación de incluir en sus condiciones generales la información exigida en el artículo 6 del Reglamento (UE) 2019/1150 sobre los bienes y servicios auxiliares ofrecidos.

p) El incumplimiento habitual por parte de los proveedores de servicios de intermediación en línea o los proveedores de motores de búsqueda en línea de la obligación de incluir en sus condiciones generales la información exigida en los apartados 1 y 2, respectivamente, con las precisiones establecidas en el apartado 3, del artículo 7 del Reglamento (UE) 2019/1150, en materia de tratamiento diferenciado de bienes o servicios.

q) El incumplimiento por parte de los proveedores de servicios de intermediación de la obligación establecida en la letra a) del artículo 8 del Reglamento (UE) 2019/1150, así como el incumplimiento habitual de las obligaciones contenidas en las letras b) y c) del citado precepto.

r) El incumplimiento habitual por parte de los proveedores de servicios de intermediación en línea de la obligación de informar sobre el acceso a datos por parte de los usuarios profesionales establecida en el artículo 9 del Reglamento (UE) 2019/1150.

s) El incumplimiento habitual por parte de los proveedores de servicios de intermediación en línea de la obligación de justificar las restricciones a la oferta de condiciones diferentes por otros medios prevista en el artículo 10 del Reglamento (UE) 2019/1150.

t) El incumplimiento por parte de los proveedores de servicios de intermediación en línea que no sean pequeñas empresas, de la obligación de establecer un sistema interno y gratuito para tramitar las reclamaciones de los usuarios profesionales, en los términos previstos por el artículo 11 del Reglamento (UE) 2019/1150.

u) El incumplimiento por parte de los proveedores de servicios de intermediación en línea que no sean pequeñas empresas, de la obligación de designar al menos dos mediadores, o de cualquier otra de las obligaciones en materia de mediación establecidas en el artículo 12 del Reglamento (UE) 2019/1150.»

Seis. Se añaden diez nuevas letras de la j) a la s) al apartado 4 del artículo 38 con la siguiente redacción:

«j) La exigencia del pago de un canon por atender la obligación prevista en el artículo 12 ter, cuando así lo permita el artículo 12.5 del Reglamento (UE) 2016/679, si su cuantía excediese el importe de los costes afrontados.

k) El incumplimiento de la obligación prevista en el artículo 12 ter, cuando no constituya infracción grave.

l) El incumplimiento por parte de los proveedores de servicios de intermediación en línea de la obligación establecida en el apartado 5 del artículo 3 del Reglamento (UE) 2019/1150 en materia de visibilidad de la identidad del usuario profesional, cuando no constituya infracción grave.

m) El incumplimiento por parte de los proveedores de servicios de intermediación en línea de cualquiera de las obligaciones en materia de restricción, suspensión y terminación del servicio establecidas en los apartados 1, 2 y 3 del artículo 4 del Reglamento (UE) 2019/1150, cuando no constituya infracción grave.

n) El incumplimiento por parte de los proveedores de servicios de intermediación en línea o proveedores de motores de búsqueda en línea de cualquiera de las obligaciones en materia de clasificación establecidas en el artículo 5 del Reglamento (UE) 2019/1150 que les resulten aplicables, cuando no constituya infracción grave.

o) El incumplimiento por parte de los proveedores de servicios de intermediación en línea de la obligación de incluir en sus condiciones generales la información exigida en el artículo 6 del Reglamento (UE) 2019/1150 sobre los bienes y servicios auxiliares ofrecidos, cuando no constituya infracción grave.

p) El incumplimiento por parte de los proveedores de servicios de intermediación en línea y los proveedores de motores de búsqueda en línea de la obligación de incluir en sus condiciones generales la información exigida en los apartados 1 y 2, respectivamente, con las precisiones establecidas en el apartado 3, del artículo 7 del Reglamento (UE) 2019/1150, en materia de tratamiento diferenciado de bienes o servicios, cuando no constituya infracción grave.

q) El incumplimiento por parte de los proveedores de servicios de intermediación en línea de las obligaciones en materia de cláusulas contractuales específicas establecidas en el artículo 8 del Reglamento (UE) 2019/1150, cuando no constituya infracción grave.

r) El incumplimiento por parte de los proveedores de servicios de intermediación en línea de la obligación de informar sobre el acceso a datos por parte de los usuarios profesionales establecida en el artículo 9 del Reglamento (UE) 2019/1150, cuando no constituya infracción grave.

s) El incumplimiento por parte de los proveedores de servicios de intermediación en línea de la obligación de justificar las restricciones a la oferta de condiciones diferentes por otros medios prevista en el artículo 10 del Reglamento (UE) 2019/1150, cuando no constituya infracción grave.»

Siete. El artículo 43 queda redactado como sigue:

«Artículo 43. *Competencia sancionadora.*

1. La imposición de sanciones por el incumplimiento de lo previsto en esta Ley corresponderá, en el caso de infracciones muy graves, a la persona titular del Ministerio de Asuntos Económicos y Transformación Digital, y en el de infracciones graves y leves, a la persona titular de la Secretaria de Estado de Digitalización e Inteligencia Artificial.

No obstante lo anterior, la imposición de sanciones por incumplimiento de las resoluciones dictadas por los órganos competentes en función de la materia o entidad de que se trate a que se refieren las letras a) y b) del artículo 38.2 de esta Ley corresponderá al órgano que dictó la resolución incumplida. Igualmente, corresponderá a la Agencia de Protección de Datos la imposición de sanciones por la comisión de las infracciones tipificadas en los artículos 38.3 c), d) e i) y 38.4 d), g) y h) de esta Ley.

2. La potestad sancionadora regulada en esta Ley se ejercerá de conformidad con lo establecido al respecto en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y en sus normas de desarrollo. El procedimiento tendrá una duración máxima de nueve meses a contar desde la fecha del acuerdo de iniciación. El plazo máximo de duración del procedimiento simplificado será de tres meses.»

Disposición final cuarta. *Modificación de la Ley 17/2009, de 23 de noviembre, sobre el libre acceso a las actividades de servicios y su ejercicio.*

Se introduce una nueva disposición adicional séptima con el siguiente contenido:

«Disposición adicional séptima. *Incumplimiento de la prohibición de discriminación.*

El incumplimiento de la prohibición de discriminación prevista en el artículo 16.3 de esta Ley y el Reglamento (UE) 2018/302 del Parlamento Europeo y del Consejo, de 28 de febrero de 2018, sobre medidas destinadas a impedir el bloqueo geográfico injustificado y otras formas de discriminación por razón de la nacionalidad, del lugar de residencia o del lugar de establecimiento de los clientes en el mercado interior y por el que se modifican los Reglamentos (CE) 2006/2004 y (UE) 2017/2394 y la Directiva 2009/22/CE, se reputará desleal a los efectos de la Ley 3/1991, de 10 de enero, de Competencia Desleal, sin perjuicio del régimen de infracciones y sanciones contenido en el Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias.»

Disposición final quinta. *Título competencial.*

Esta Ley se dicta al amparo de las competencias exclusivas que corresponden al Estado en materia de legislación civil, telecomunicaciones y seguridad pública, conforme a lo dispuesto en el artículo 149.1.8.ª, 21.ª y 29.ª de la Constitución Española.

El artículo 3 y la disposición final segunda se dictan, además, al amparo de lo previsto en el artículo 149.1.6.ª de la Constitución, el cual atribuye al Estado competencia exclusiva en materia de legislación procesal. Por su parte la disposición adicional segunda se dicta al amparo de lo previsto en el artículo 149.1.18.ª de la Constitución, en relación con la competencia estatal exclusiva sobre las bases del régimen jurídico de las Administraciones públicas y el procedimiento administrativo común.

Disposición final sexta. *Desarrollo reglamentario.*

Se habilita al Gobierno para dictar las disposiciones reglamentarias que sean precisas para el desarrollo y aplicación de esta Ley.

Disposición final séptima. *Entrada en vigor.*

La presente Ley entrará en vigor al día siguiente al de su publicación en el «Boletín Oficial del Estado».

§ 39

Ley 9/2014, de 9 de mayo, General de Telecomunicaciones. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 114, de 10 de mayo de 2014
Última modificación: 29 de junio de 2022
Referencia: BOE-A-2014-4950

Norma derogada, a excepción de su disposición adicional decimosexta y las disposiciones transitorias séptima, novena y duodécima, con efectos de 30 de junio de 2022, por la disposición derogatoria única.a) de la Ley 11/2022, de 28 de junio, sin perjuicio de lo dispuesto en sus disposiciones transitorias. Ref. BOE-A-2022-10757

[. . .]

Disposición adicional decimosexta. *La entidad pública empresarial Red.es.*

1. La entidad Red.es, creada por la disposición adicional sexta de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, se configura como entidad pública empresarial, conforme a lo previsto en el artículo 43.1.b) de la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado. Dicha entidad queda adscrita al Ministerio de Industria, Energía y Turismo, a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información.

2. La entidad pública empresarial Red.es tiene personalidad jurídica propia, plena capacidad de obrar y patrimonio propio y se regirá por lo establecido en esta disposición adicional, en su propio Estatuto, en la citada Ley 6/1997 y en las demás normas que le sean de aplicación.

3. Constituye el objeto de la entidad pública empresarial la gestión, administración y disposición de los bienes y derechos que integran su patrimonio, correspondiéndole la tenencia, administración, adquisición y enajenación de los títulos representativos del capital de las sociedades en las que participe o pueda participar en el futuro. La entidad pública empresarial actuará, en cumplimiento de su objeto, conforme a criterios empresariales.

Para el cumplimiento de su objeto, la entidad pública empresarial podrá realizar toda clase de actos de administración y disposición previstos en la legislación civil y mercantil. Asimismo, podrá realizar cuantas actividades comerciales o industriales estén relacionadas con dicho objeto, conforme a lo acordado por sus órganos de gobierno. Podrá actuar, incluso, mediante sociedades por ella participadas.

La entidad pública empresarial Red.es contará además con las siguientes funciones:

a) La gestión del registro de los nombres y direcciones de dominio de internet bajo el código de país correspondiente a España (.es), de acuerdo con la política de registros que

se determine por el Ministerio de Industria, Energía y Turismo y en la normativa correspondiente.

b) La participación en los órganos que coordinen la gestión de Registros de nombre y dominios de la Corporación de Internet para la Asignación de Nombres y Números (ICANN), o la organización que en su caso la sustituya, así como el asesoramiento al Ministerio de Industria, Energía y Turismo en el Comité Asesor Gubernamental de ICANN (GAC) y, en general cuando le sea solicitado, el asesoramiento a la Administración General del Estado en el resto de los organismos internacionales y, en particular, en la Unión Europea, en todos los temas de su competencia.

c) La de observatorio del sector de las telecomunicaciones y de la sociedad de la información.

d) La elaboración de estudios e informes y, en general, el asesoramiento de la Administración General del Estado en todo lo relativo a la sociedad de la información, de conformidad con las instrucciones que dicte el Ministerio de Industria, Energía y Turismo.

e) El fomento y desarrollo de la Sociedad de la Información.

4. El régimen de contratación, de adquisición y de enajenación de la entidad se acomodará a las normas establecidas en derecho privado, sin perjuicio de lo determinado en el texto refundido de la Ley de Contratos del Sector Público, aprobado por el real decreto Legislativo 3/2011, de 14 de noviembre.

5. El régimen patrimonial de la entidad pública empresarial se ajustará a las previsiones del artículo 56 de la Ley 6/1997. No obstante, los actos de disposición y enajenación de los bienes que integran su patrimonio se regirán por el derecho privado. En especial, la entidad pública empresarial Red.es podrá afectar sus activos a las funciones asignadas a la misma en la letra e) del apartado tercero de esta disposición y a financiar transitoriamente el déficit de explotación resultante entre los ingresos y gastos correspondientes a las funciones asignadas en las letras a), b), c) y d) del mismo apartado.

6. La contratación del personal por la entidad pública empresarial se ajustará al derecho laboral, de acuerdo con las previsiones contenidas en el artículo 55 de la Ley 6/1997, debiéndose respetar, en cualquier caso, los principios de igualdad, mérito y capacidad.

7. El régimen presupuestario, el económico-financiero, el de contabilidad, el de intervención y el de control financiero de la entidad pública empresarial será el establecido en la Ley General Presupuestaria, de acuerdo con lo previsto en el artículo 58 y en la disposición transitoria tercera de la Ley 6/1997.

8. Los recursos económicos de la entidad podrán provenir de cualquiera de los enumerados en el apartado 1 del artículo 65 de la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado. Entre los recursos económicos de la entidad pública empresarial Red.es se incluyen los ingresos provenientes de lo recaudado en concepto del precio público por las operaciones de registro relativas a los nombres de dominio de Internet bajo el código de país correspondiente a España «.es» regulado en el apartado siguiente.

9. Precios Públicos por asignación, renovación y otras operaciones registrales de los nombres de dominio bajo el «.es».

La contraprestación pecuniaria que se satisfaga por la asignación, renovación y otras operaciones registrales realizadas por la entidad pública empresarial Red.es en ejercicio de su función de Autoridad de Asignación de los nombres de dominio de Internet bajo el código de país correspondiente a España tendrán la consideración de precio público.

Red.es, previa autorización del Ministerio de Industria, Energía y Turismo, establecerá mediante la correspondiente Instrucción, las tarifas de los precios públicos por la asignación, renovación y otras operaciones de registro de los nombres de dominio bajo el «.es». La propuesta de establecimiento o modificación de la cuantía de precios públicos irá acompañada, de conformidad con lo previsto en el artículo 26 de la Ley 8/1989, de 13 de abril, que regula el Régimen Jurídico de las Tasas y Precios Públicos, de una memoria económico-financiera que justificará el importe de los mismos que se proponga y el grado de cobertura financiera de los costes correspondientes.

La gestión recaudatoria de los precios públicos referidos en este apartado corresponde a la entidad pública empresarial Red.es que determinará el procedimiento para su liquidación y

pago mediante la Instrucción mencionada en el párrafo anterior en la que se establecerán los modelos de declaración, plazos y formas de pago.

La entidad pública empresarial Red.es podrá exigir la anticipación o el depósito previo del importe total o parcial de los precios públicos por las operaciones de registro relativas a los nombres de dominio «.es».

[. . .]

Disposición transitoria séptima. *Solicitudes de autorizaciones o licencias administrativas efectuadas con anterioridad.*

1. Los procedimientos iniciados con anterioridad a la entrada en vigor de la presente Ley, y que tengan por finalidad la obtención de las licencias o autorizaciones de obra, instalaciones, de funcionamiento o de actividad, o de carácter medioambiental u otras de clase similar o análogas que fuesen precisas con arreglo a la normativa anterior, se tramitarán y resolverán por la normativa vigente en el momento de la presentación de la solicitud.

2. No obstante lo dispuesto en el apartado anterior, el interesado podrá, con anterioridad a la resolución, desistir de su solicitud y, de este modo, optar por la aplicación de la nueva normativa en lo que ésta a su vez resultare de aplicación.

[. . .]

Disposición transitoria novena. *Adaptación de la normativa y los instrumentos de planificación territorial o urbanística elaborados por las administraciones públicas competentes que afecten al despliegue de las redes públicas de comunicaciones electrónicas.*

La normativa y los instrumentos de planificación territorial o urbanística elaborados por las administraciones públicas competentes que afecten al despliegue de las redes públicas de comunicaciones electrónicas deberán adaptarse a lo establecido en los artículos 34 y 35 en el plazo máximo de un año desde la entrada en vigor de la presente Ley.

[. . .]

Disposición transitoria duodécima. *Régimen transitorio de las estaciones o infraestructuras radioeléctricas para la prestación de servicios de comunicaciones electrónicas disponibles para el público para cuya instalación se hubiera presentado solicitud de licencia o autorización.*

Las estaciones o infraestructuras radioeléctricas para la prestación de servicios de comunicaciones electrónicas disponibles para el público para cuya instalación se hubiera solicitado la licencia o autorización previa de instalaciones, de funcionamiento, de actividad, de carácter medioambiental u otras de clase similar o análogas a las que se refiere el artículo 34.6, podrán continuar instaladas y en funcionamiento, sin perjuicio de que las administraciones públicas competentes puedan ejercer las potestades administrativas de comprobación, inspección, sanción y, en general, de control, que tengan atribuidas y que están referidas en el citado artículo 34.6 así como en el artículo 5 de la Ley 12/2012, de 26 de diciembre, de Medidas Urgentes de Liberalización del Comercio y Determinados Servicios.

No obstante, y de conformidad con lo prevenido en la disposición transitoria de la mencionada Ley 12/2012, de 26 de diciembre, los prestadores de servicios de comunicaciones electrónicas para el público que hubieren solicitado las licencias o autorizaciones anteriormente mencionadas, sin perjuicio de la continuidad y funcionamiento de las respectivas instalaciones, podrán desistir de dichas solicitudes en curso y optar por presentar declaraciones responsables o, en su caso, comunicaciones previas de cambio de titularidad en los términos previstos en la citada Ley.

El ejercicio de las potestades administrativas de comprobación, inspección, sanción y, en general, de control deberá respetar los parámetros y requerimientos técnicos esenciales necesarios para garantizar el funcionamiento de las distintas redes y servicios de

comunicaciones electrónicas mencionados en el artículo 34.4 y en la disposición adicional undécima.

[. . .]

§ 40

Ley 11/2022, de 28 de junio, General de Telecomunicaciones

Jefatura del Estado
«BOE» núm. 155, de 29 de junio de 2022
Última modificación: 28 de junio de 2023
Referencia: BOE-A-2022-10757

FELIPE VI

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley:

PREÁMBULO

I

La Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, introdujo reformas estructurales en el régimen jurídico de las telecomunicaciones dirigidas a facilitar el despliegue de redes y la prestación de servicios por parte de los operadores. Dicha ley estableció las bases para asegurar que la extensión de las redes de nueva generación se llevase a cabo conforme a los principios de fomento de la inversión e impulso de la competencia, garantizando un marco regulatorio claro y estable, que ha proporcionado seguridad jurídica y eliminado barreras que dificultaban el despliegue de redes. Ello ha permitido a los operadores ofrecer a los usuarios servicios innovadores, de mayor calidad y cobertura, a precios competitivos y con mejores condiciones, contribuyendo de este modo a potenciar la competitividad y la productividad de la economía española en su conjunto.

En la actualidad, las redes alcanzan en nuestro país una cobertura del 95,2 por ciento de la población para una velocidad de acceso de 30 Mbps y del 87,6 por ciento para una velocidad de acceso de 100 Mbps, situando a España en una posición buena en el ámbito europeo en lo que se refiere a infraestructuras de conectividad de banda ancha, tal como reconoce la Comisión Europea en su «Índice de la Sociedad y la Economía Digitales 2020 (DESI)» en el que se indica que el despliegue de redes de fibra óptica (FTTP) sigue siendo una característica importante del mercado digital español, con una cobertura del 95,2 por ciento de los hogares, muy por encima de la media de la UE que se sitúa en el 34 por ciento. De acuerdo con datos del Observatorio Nacional del Sector de las Telecomunicaciones y de la Sociedad de la Información, el volumen de negocio del sector de las telecomunicaciones en España se situó en torno a los 28.337 millones de euros en 2020, suponiendo el sector de las Tecnologías de la Información y el Conocimiento el 3,23 por ciento del PIB nacional y

dando empleo a 446.881 personas. Además, según datos de evolución del mercado de la Comisión Nacional de los Mercados y la Competencia, existe un elevado grado de despliegue por parte de diferentes operadores en el mercado español.

En estos momentos de incertidumbre internacional, las telecomunicaciones constituyen uno de los sectores más dinámicos de la economía y uno de los que más pueden contribuir, por su carácter transversal, al crecimiento, la productividad y a la generación de empleo, situándose asimismo como palanca de la transformación digital y ecológica y como motor del desarrollo sostenible y el bienestar social.

Con ocasión de la declaración de la pandemia por COVID-19, se ha demostrado que las telecomunicaciones no solo garantizan la prestación de servicios muy necesarios como son el teletrabajo, la telemedicina o la enseñanza online, sino que también favorecen el crecimiento de otros sectores como la industria de los contenidos, el almacenamiento y procesamiento de datos en la nube, el «Internet de las Cosas» o la automoción conectada.

Las telecomunicaciones son también un elemento de impulso a la transición ecológica hacia un nuevo modelo económico y social basado en la eficiencia energética, la movilidad sostenible y la economía circular, dado que al ser un sector que genera un bajo nivel de emisiones relativo, su papel puede ser fundamental en la lucha frente al cambio climático al facilitar un uso más eficiente de los recursos energéticos en otros sectores.

En este sentido, la computación en centros de datos se ha incrementado en más de un 500 por ciento entre los años 2010 y 2018, mientras que el consumo de energía eléctrica por este sector solo ha aumentado un 6 por ciento y es evidente, por ejemplo, que durante la pandemia la traslación de actividad social a las infraestructuras digitales ha supuesto una sustancial mejora de la calidad del aire y del medio ambiente.

Las redes de muy alta capacidad, y en especial la nueva generación de telefonía móvil 5G, son claves para cumplir con los ambiciosos objetivos de descarbonización y reducción de emisiones de gases de efecto invernadero asumidos en el ámbito europeo para el año 2030, ya que facilitan la aparición de nuevos servicios inteligentes máquina a máquina (redes eléctricas inteligentes, logística inteligente, ciudades inteligentes, sistemas de producción inteligente) y la sustitución de determinadas actividades físicas por otras virtuales, evitando desplazamientos innecesarios y contribuyendo a la implantación de nuevas fuentes de energía limpias y renovables.

Dicho proceso de virtualización de la economía supondría la sustitución de procesos, desplazamientos, reuniones y viajes por alternativas virtuales de bajas emisiones con objeto de apostar por salas de reuniones virtuales a las que conectarse a través de las comunicaciones electrónicas, fomentar el uso de productos de telecomunicaciones para que los empleados puedan trabajar a distancia desde su casa o utilizar las comunicaciones móviles para mejorar los procesos de comercio electrónico y facilitar los sistemas de pedido y entrega de las compras. Estas iniciativas no solo permitirían adaptarnos a eventuales medidas de contención sanitaria ante posibles epidemias, sino que también lograrían reducir las emisiones de CO_2 en Europa en más de 22 millones de toneladas, así como un ahorro potencial en consumo energético de 14.100 millones de euros (en España, la reducción alcanzaría los 2 millones de toneladas de emisiones de CO_2, y el ahorro hasta 1.330 millones de euros).

Por tanto, el sector de las comunicaciones electrónicas supone una indudable contribución claramente positiva a la descarbonización de la economía.

Por otro lado, el establecimiento de las nuevas redes, al ser palanca de vertebración territorial, puede ayudar a la fijación de la población en el territorio, combatiendo la despoblación rural, lo que, según el Informe sobre el uso de la tierra y el cambio climático, elaborado en 2019, por el Panel Intergubernamental de Expertos en Cambio Climático (IPCC en adelante) de la ONU, constituye uno de los medios más eficaces para luchar contra los efectos del cambio climático.

El despliegue de nuevas redes en el medio rural, en especial en los territorios con gran dispersión poblacional y complicada orografía, resulta imprescindible para posibilitar un adecuado desarrollo económico y fomentar el emprendimiento y la creación de empleo.

En cuanto a los efectos económicos de la tecnología 5G, los análisis de la Comisión Europea sobre los beneficios estimados de su introducción en cuatro sectores productivos (automoción, salud, transporte y utilities) prevén un aumento progresivo hasta alcanzar los

62.500 millones de euros de impacto directo anual dentro de la Unión Europea en 2025, lo que se elevaría a 113.000 millones de euros si se suman los impactos indirectos. El mismo estudio estima que en nuestro país se obtendrían unos beneficios indirectos en los cuatro sectores analizados de 14.600 millones de euros y una importante creación de empleo.

II

La aprobación de esta ley constituye una de las medidas incluidas en el Plan de Recuperación, Transformación y Resiliencia de la economía española (PRTR), aprobado por la Comisión Europea el día 16 de junio de 2021, con el objetivo a corto plazo de apoyar la recuperación de la economía española tras la crisis sanitaria, impulsar a medio plazo un proceso de transformación estructural y lograr a largo plazo un desarrollo más sostenible y resiliente desde el punto de vista económico financiero.

Con esta medida incluida dentro de la Componente 15 del PRTR «Conectividad digital, impulso a la ciberseguridad y despliegue del 5G» se pretende la tramitación y aprobación de una nueva Ley General de Telecomunicaciones, transposición de la Directiva 2018/1972 del Código Europeo de Comunicaciones Electrónicas.

En concreto, la aprobación de esta ley constituye la ejecución de la medida C15.R1 del PRTR consistente en la «Reforma del marco normativo de telecomunicaciones: Ley General, instrumentos regulatorios e Instrumentos de aplicación».

En cumplimiento de lo dispuesto en el Plan de Recuperación, Transformación y Resiliencia, en el Reglamento (UE) 2021/241 del Parlamento Europeo y del Consejo, de 12 de febrero de 2021, por el que se establece el Mecanismo de Recuperación y Resiliencia, y su normativa de desarrollo, en particular la Comunicación de la Comisión Guía técnica (2021/C 58/01) sobre la aplicación del principio de «no causar un perjuicio significativo», así como lo requerido en la Decisión de Ejecución del Consejo relativa a la aprobación de la evaluación del Plan de Recuperación, Transformación y Resiliencia de España (CID) y su documento anexo, todas las actuaciones que se lleven a cabo en cumplimiento de la presente ley deben respetar el principio de no causar un perjuicio significativo al medioambiente (principio DNSH por sus siglas en inglés, «Do No Significant Harm»). Ello incluye el cumplimiento de las condiciones específicas asignadas en la Componente 15, así como en la medida R1 en la que se enmarcan dichas actuaciones en lo referido al principio DNSH y especialmente las recogidas en los apartados 3 y 8 del documento del Componente del Plan y en el anexo a la CID.

Igualmente, la aprobación de esta ley constituye una de las principales medidas del Plan España Digital 2025, presentado por el Gobierno el 24 de julio de 2020, y que tiene por objetivo impulsar el proceso de transformación digital del país, de forma alineada con la estrategia digital de la Unión Europea, mediante la colaboración público-privada y con la participación de todos los agentes económicos y sociales.

En concreto, dicho Plan pretende movilizar 140.000 millones de euros de inversión pública y privada durante los próximos cinco años, a fin de impulsar la digitalización de la economía española.

España Digital 2025 centra sus objetivos en el impulso a la transformación digital del país como una de las palancas fundamentales para relanzar el crecimiento económico, la reducción de la desigualdad, el aumento de la productividad y el aprovechamiento de las oportunidades que brindan las nuevas tecnologías, con respeto a los valores constitucionales y europeos, y la protección de los derechos individuales y colectivos.

El Plan consta de unas 50 medidas que se articulan en torno a diez ejes estratégicos. El primero es el eje de la conectividad digital, encuadrándose como medida número 2 la aprobación de una nueva Ley General de Telecomunicaciones, la cual tiene como objetivo fundamental la transposición al ordenamiento jurídico español de la Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2018, por la que se establece el Código Europeo de las Comunicaciones Electrónicas (en adelante, el Código).

El Código sitúa a las comunicaciones electrónicas como pilar de la transformación digital de la economía, la cual es uno de los ejes prioritarios de la política europea para la recuperación sostenible tras la pandemia por COVID-19, tal y como se refleja en el Plan de recuperación y en el marco financiero plurianual 2021-2027, acordado por los líderes de la Unión Europea el 21 de julio de 2020.

El Código refunde y actualiza, conforme a la Estrategia de Mercado Único Digital del año 2015, en un único texto, el paquete de Directivas comunitarias del año 2002 (modificadas en el año 2009), la Directiva 2002/19/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión (Directiva acceso),la Directiva 2002/20/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a la autorización de redes y servicios de comunicaciones electrónicas (Directiva autorización), la Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas (Directiva marco), la Directiva 2002/22/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas (Directiva servicio universal).

El Código no refunde la Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) por cuanto se encuentra en tramitación un proyecto de Reglamento sobre esta materia, dirigido a actualizar y sustituir a la Directiva actualmente vigente. No obstante, la presente ley sí recoge lo establecido en dicha Directiva que sigue estando vigente. Esta ley aborda también otros aspectos incluidos dentro del concepto amplio de telecomunicaciones, de forma que incluye las novedades que en materia de equipos radioeléctricos introdujo la Directiva 2014/53/UE, del Parlamento Europeo y del Consejo, de 16 de abril de 2014, relativa a la armonización de las legislaciones de los Estados Miembros sobre la comercialización de equipos radioeléctricos y por la que se deroga la Directiva 1999/5/CE (Directiva RED) transpuesta al ordenamiento jurídico español por Real Decreto 188/2016, de 6 de mayo, por el que se aprueba el Reglamento por el que se establecen los requisitos para la comercialización, puesta en servicio y uso de equipos radioeléctricos, y se regula el procedimiento para la evaluación de conformidad, la vigilancia del mercado y el régimen sancionador de los equipos de telecomunicación, que mantiene su vigencia, en desarrollo de lo establecido en el título IV.

Asimismo, y aunque se trata de normativa directamente aplicable o que ya ha sido transpuesta al ordenamiento jurídico español, a fin de introducir coherencia y seguridad jurídica, se incluyen también en esta ley general del sector, los principales aspectos de la normativa contenida en el Real Decreto 330/2016, de 9 de septiembre, relativo a medidas para reducir el coste de despliegue de las redes de comunicaciones electrónicas de alta velocidad, por el que se transpone la Directiva 2014/61/UE, de 15 de mayo de 2014 (Directiva BBCost, en adelante), que mantiene también su vigencia como norma de desarrollo, las garantías sobre neutralidad de red incorporadas al Reglamento (UE) 2015/2120, del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, por el que se establecen medidas en relación con el acceso a una internet abierta y tarifas al por menor para comunicaciones intracomunitarias reguladas y se modifican la Directiva 2002/22/CE y el Reglamento (UE) 531/2012 (Reglamento TSM), así como determinados aspectos de la Directiva 2014/30/UE, del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, sobre la armonización de las legislaciones de los Estados miembros en materia de compatibilidad electromagnética y del Reglamento (UE) 531/2012, del Parlamento Europeo y del Consejo, de 13 de junio de 2012, relativo a la itinerancia en las redes públicas de comunicaciones móviles en la Unión.

III

El principal objetivo de la ley es el fomento de la inversión en redes de muy alta capacidad, introduciendo figuras como la de los estudios geográficos o la de la coinversión, lo que podrá tenerse en cuenta en el ámbito de los análisis de mercado. Con este mismo objetivo de incentivar los despliegues se garantiza la utilización compartida del dominio público o la propiedad privada, el uso compartido de las infraestructuras y recursos asociados y la utilización compartida de los tramos finales de las redes de acceso.

También se introducen importantes novedades en materia de dominio público radioeléctrico, incorporando medidas que facilitan el uso compartido del espectro

radioeléctrico por operadores y evitando restricciones indebidas a la implantación de puntos de acceso inalámbrico para pequeñas áreas.

Adicionalmente, con el ánimo de promover la previsibilidad regulatoria y la recuperación de las inversiones, se amplían los plazos de duración mínimos y máximos de las concesiones de uso privativo del dominio público radioeléctrico con limitación de número, de manera que estas concesiones tendrán una duración mínima de veinte años y podrán tener una duración máxima, si se otorga el plazo máximo de prórroga, de hasta cuarenta años.

La ley incorpora, asimismo, avances en materia de protección de los derechos de los usuarios finales de los servicios de telecomunicaciones, reforzando, por ejemplo, las obligaciones de transparencia y regulando los contratos empaquetados.

Además, se revisa la normativa sobre acceso y análisis de mercado, se actualiza la normativa sobre servicio universal de telecomunicaciones y se introducen medidas en materia de seguridad destinadas a gestionar los nuevos riesgos a los que se ven sometidos las redes y los servicios.

Recoge, conforme al Código, la posibilidad de que la Comisión Europea establezca tarifas únicas máximas de terminación de llamadas de voz a escala europea, y se refuerza el funcionamiento del número 112 como número de llamada de emergencia en toda Europa, estableciendo la obligación de que dicho número sea accesible a personas con discapacidad. Se introduce, asimismo un sistema de alertas públicas a través de los servicios móviles en caso de grandes catástrofes o emergencias inminentes o en curso.

Por último, se incorpora a la ley la clasificación de los servicios de comunicaciones electrónicas contenida en el Código. De esta forma, se distingue entre servicios de acceso a internet, servicios de comunicaciones interpersonales y servicios consistentes, en su totalidad o principalmente, en el transporte de señales, como son los servicios de transmisión utilizados para la prestación de servicios máquina a máquina y para la radiodifusión. A su vez, dentro de los servicios de comunicaciones interpersonales se diferencian los servicios de comunicaciones interpersonales basados en numeración y los servicios de comunicaciones interpersonales independientes de la numeración, según permitan o no, respectivamente comunicaciones con recursos de numeración pública asignados, es decir, de un número o números de los planes de numeración nacional o internacional.

IV

La ley consta de ciento catorce artículos, agrupados en ocho títulos, treinta disposiciones adicionales, siete disposiciones transitorias, una disposición derogatoria, seis disposiciones finales y tres anexos.

El título I, «Disposiciones generales», establece el objeto de la ley, que aborda, de forma integral, el régimen de las «telecomunicaciones» al amparo de la competencia exclusiva estatal establecida en el artículo 149.1.21.ª de la Constitución Española.

La ley excluye expresamente de su regulación los contenidos difundidos a través de servicios de comunicación audiovisual, que constituyen parte del régimen de los medios de comunicación social, así como los servicios de intercambio de vídeos a través de plataforma. No obstante, las redes utilizadas como soporte de estos servicios y los recursos asociados sí son parte integrante de las comunicaciones electrónicas reguladas en esta ley.

Igualmente, queda excluida de la regulación de esta ley la prestación de servicios sobre las redes de telecomunicaciones que no consistan principalmente en el transporte de señales a través de dichas redes, la cual se regula en la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

En relación con los objetivos y principios, la ley reordena los ya enumerados en la anterior ley, contribuyendo a su mejor comprensión y a una mejor visualización de aquellos que deben ser considerados como prioritarios. Asimismo, añade determinados principios nuevos como el de promover la conectividad y el acceso a las redes de muy alta capacidad, así como su adopción por los ciudadanos y empresas.

Por último, se establecen aquellos servicios de telecomunicaciones que tienen la consideración de servicio público como son los servicios de telecomunicaciones para la seguridad y defensa nacionales, la seguridad pública, la seguridad vial y la protección civil.

El título II regula el régimen general de suministro de redes y de prestación de servicios y establece que la habilitación para instalar y explotar redes o prestar servicios en régimen de libre competencia, viene concedida con carácter general e inmediato por la ley, con el único requisito de notificación al Registro de operadores, dependiente de la Comisión Nacional de los Mercados y la Competencia. No obstante, para evitar distorsiones a la competencia que puedan derivarse de la participación de operadores públicos en el mercado de comunicaciones electrónicas, la ley establece limitaciones concretas para la instalación y explotación de redes y la prestación de servicios por parte de las Administraciones públicas.

El título II recoge asimismo el derecho de acceso de los operadores a redes y recursos asociados y regula la interconexión y las obligaciones que, de acuerdo con la normativa de la Unión Europea, pudiera llegar a imponer la Comisión Nacional de los Mercados y la Competencia a los operadores con peso significativo en el ámbito de regulación *ex ante* de los mercados.

Por último, este título regula las competencias de la Comisión Nacional de los Mercados y la Competencia en materia de resolución de conflictos entre operadores y el derecho de acceso de los operadores a la numeración.

El título III, relativo a obligaciones de servicio público y derechos y obligaciones de carácter público en la instalación y explotación de redes y en la prestación de servicios de comunicaciones electrónicas, obliga a las Administraciones públicas a que el planeamiento urbanístico prevea la necesaria dotación de infraestructuras de telecomunicaciones y garantiza, de acuerdo con la citada Directiva BBCost, el derecho de acceso de los operadores a infraestructuras de Administraciones públicas y a infraestructuras lineales como electricidad, gas, agua, saneamiento o transporte, estableciendo, con carácter general, un régimen de declaración responsable en relación con los despliegues, reduciendo los tiempos de respuesta y las cargas administrativas relacionadas con los mismos.

Asimismo, se recogen en este título III las obligaciones de servicio universal y las relacionadas con la integridad y seguridad de las redes, así como los derechos de los usuarios de las telecomunicaciones y las garantías de acceso a las comunicaciones de emergencia y al número 112, de emergencias de ámbito europeo.

En relación con los derechos de los usuarios de comunicaciones electrónicas es de significar que su protección viene garantizada además de por las disposiciones específicas establecidas en esta ley, que regulan los derechos específicos de los usuarios de comunicaciones electrónicas, que se refuerzan en esta ley, por la normativa general de protección de los derechos de consumidores y usuarios. Las disposiciones que esta ley y su desarrollo reglamentario contiene en materia de derechos específicos de los usuarios finales y consumidores de servicios de comunicaciones electrónicas serán de aplicación preferente a las disposiciones que regulen con carácter general los derechos de los consumidores y usuarios. Esta complementariedad de normativas convierte a las telecomunicaciones en uno de los sectores cuyos usuarios gozan de un mayor nivel de protección, tal como ha destacado de manera expresa la jurisprudencia del Tribunal Constitucional (STC 72/2014).

En este ámbito de reconocimiento y protección de los derechos de los usuarios de comunicaciones electrónicas ha de afirmarse que esta ley está en línea con la Carta de Derechos Digitales presentada por el Gobierno el 14 de julio de 2021, como marco para la producción normativa y las políticas públicas que garantice la protección de los derechos individuales y colectivos ante las nuevas situaciones y circunstancias generadas en el entorno digital.

En la presente ley se incluyen mecanismos de colaboración entre el Ministerio de Asuntos Económicos y Transformación Digital y las Administraciones públicas, dirigidos a facilitar y fomentar la instalación y explotación de las redes públicas de comunicaciones electrónicas. Así, el conjunto de Administraciones públicas debe facilitar el despliegue de infraestructuras de redes de comunicaciones electrónicas en su ámbito territorial, para lo que deben dar debido cumplimiento a los deberes de información recíproca y de colaboración y cooperación mutua en el ejercicio de sus actuaciones y competencias. Pese a ello, en ocasiones el acuerdo puede no resultar posible, por lo que la propia ley prevé mecanismos para solucionar los desacuerdos, como que finalmente el Gobierno pueda autorizar la ubicación o el itinerario concreto de una infraestructura de red de comunicaciones electrónicas, si bien en este caso, habida cuenta de las especialidades que rodean la

instalación de una red de comunicaciones electrónicas, y en aras de respetar las competencias de otras Administraciones públicas, se establece la necesidad de tener en cuenta ciertos aspectos que condicionan el ejercicio de dicha potestad, siempre y cuando se garantice el despliegue efectivo de la red.

En el título IV, relativo a los equipos de telecomunicación, se regulan los requisitos esenciales que han de cumplir estos equipos, la evaluación de su conformidad con dichos requisitos y la vigilancia del mercado, estableciéndose, además, las condiciones que deben cumplir las instalaciones y los instaladores.

En relación con la administración del dominio público radioeléctrico, el título V introduce como objetivo del uso del espectro lograr la cobertura del territorio nacional y de la población y de los corredores nacionales y europeos así como la previsibilidad para favorecer inversiones a largo plazo. Para ello, racionaliza la adjudicación y gestión del dominio público radioeléctrico, establece medidas que faciliten el uso compartido del espectro por operadores móviles y eviten restricciones indebidas a la implantación de puntos de acceso inalámbrico para pequeñas áreas y prevé una duración mínima de las concesiones para banda ancha inalámbrica de veinte años.

El título VI, bajo la rúbrica «La administración de las telecomunicaciones» determina las competencias que tiene atribuidas la Comisión Nacional de los Mercados y la Competencia como Autoridad Nacional de Reglamentación independiente y las que corresponden al Ministerio de Asuntos Económicos y Transformación Digital como Autoridad Competente.

En el título VII, «Tasas en materia de telecomunicaciones» se mantiene la regulación anterior con algunas mejoras derivadas de la experiencia adquirida en su aplicación.

El título VIII, relativo a inspección y régimen sancionador, mantiene y refuerza las potestades inspectoras, recoge la tipificación de infracciones y la clasificación y cuantía de las sanciones, proporcionando criterios para la determinación de la cuantía de la sanción, y facilitando la adopción de medidas cautelares que podrán acordarse incluso antes de iniciar el expediente sancionador.

Las disposiciones adicionales se refieren entre otras cuestiones a la interoperabilidad de receptores de servicios de comunicación audiovisual radiofónicos para automóviles, de receptores de servicios de radio de consumo y equipos de consumo utilizados para la televisión digital, la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación o la coordinación de las ayudas públicas a la banda ancha y al desarrollo de la economía y empleo digitales y nuevos servicios digitales.

Por su parte, las disposiciones transitorias regulan diferentes aspectos que facilitarán la transición hacia la aplicación de esta nueva ley, como los planes de precios del servicio universal o el régimen transitorio para la fijación de las tasas.

En las disposiciones finales se modifica la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y se hace referencia a los títulos competenciales, a la habilitación para el desarrollo reglamentario, a la incorporación de derecho europeo y la entrada en vigor.

Finalmente, los anexos se refieren a las tasas en materia de Telecomunicaciones, a las definiciones de términos recogidos en la ley y al conjunto mínimo de los servicios que deberá soportar el servicio de acceso adecuado a internet de banda ancha.

TÍTULO I

Disposiciones generales

Artículo 1. *Objeto y ámbito de aplicación.*

1. El objeto de esta ley es la regulación de las telecomunicaciones, que comprende la instalación y explotación de las redes de comunicaciones electrónicas, la prestación de los servicios de comunicaciones electrónicas, sus recursos y servicios asociados, los equipos radioeléctricos y los equipos terminales de telecomunicación, de conformidad con el artículo 149.1.21.ª de la Constitución.

En particular, esta ley es de aplicación al dominio público radioeléctrico utilizado por parte de todas las redes de comunicaciones electrónicas, ya sean públicas o no, y con independencia del servicio que haga uso del mismo.

2. Quedan excluidos del ámbito de esta ley los servicios de comunicación audiovisual, los servicios de intercambio de vídeos a través de plataforma, los contenidos audiovisuales transmitidos a través de las redes, así como el régimen básico de los medios de comunicación social de naturaleza audiovisual a que se refiere el artículo 149.1.27.ª de la Constitución.

Asimismo, se excluyen del ámbito de esta ley los servicios que suministren contenidos transmitidos mediante redes y servicios de comunicaciones electrónicas, las actividades que consistan en el ejercicio del control editorial sobre dichos contenidos y los servicios de la Sociedad de la Información, regulados en la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, en tanto en cuanto no sean asimismo servicios de comunicaciones electrónicas.

Artículo 2. *Las telecomunicaciones como servicios de interés general.*

1. Las telecomunicaciones son servicios de interés general que se prestan en régimen de libre competencia.

2. Sólo tienen la consideración de servicio público o están sometidos a obligaciones de servicio público los servicios regulados en el artículo 4 y en el título III, respectivamente.

Artículo 3. *Objetivos y principios de la ley.*

Los objetivos y principios de esta ley son los siguientes:

a) fomentar la competencia efectiva y sostenible en los mercados de telecomunicaciones para potenciar al máximo los intereses y beneficios para las empresas y los consumidores, principalmente en términos de bajada de los precios, calidad de los servicios, variedad de elección e innovación, teniendo debidamente en cuenta la variedad de condiciones en cuanto a la competencia y los consumidores que existen en las distintas áreas geográficas, y velando por que no exista falseamiento ni restricción de la competencia en la explotación de redes o en la prestación de servicios de comunicaciones electrónicas, incluida la transmisión de contenidos;

b) desarrollar la economía y el empleo digital, promover el desarrollo del sector de las telecomunicaciones y de todos los nuevos servicios digitales que las nuevas redes de alta y muy alta capacidad permiten, impulsando la cohesión social y territorial, mediante la mejora y extensión de las redes, especialmente las de muy alta capacidad, así como la prestación de los servicios de comunicaciones electrónicas y el suministro de los recursos asociados a ellas;

c) promover, en aras a la consecución del fin de interés general que supone, el despliegue de redes y la prestación de servicios de comunicaciones electrónicas, fomentando la conectividad, el acceso a las redes de muy alta capacidad, incluidas las redes fijas, móviles e inalámbricas y la interoperabilidad de extremo a extremo, en condiciones de igualdad y no discriminación;

d) impulsar la innovación en el despliegue de redes y la prestación de servicios de comunicaciones, en aras a garantizar el servicio universal y la reducción de la desigualdad en el acceso a internet y las Tecnologías de la Información y la Comunicación (TIC), con especial consideración al despliegue de redes y servicios a la ciudadanía vinculados a la mejora del acceso funcional a internet, del teletrabajo, del medioambiente, de la salud y la seguridad públicas y de la protección civil; así como cuando faciliten la vertebración y cohesión social y territorial o contribuyan a la sostenibilidad de la logística urbana.

e) promover el desarrollo de la ingeniería, así como de la industria de productos y equipos de telecomunicaciones;

f) contribuir al desarrollo del mercado interior de servicios de comunicaciones electrónicas en la Unión Europea, facilitando la convergencia de las condiciones que permitan la inversión en redes de comunicaciones electrónicas y en su suministro, en servicios de comunicaciones electrónicas, en recursos asociados y servicios asociados en toda la Unión;

g) promover la inversión eficiente en materia de infraestructuras, especialmente en las redes de muy alta capacidad, incluyendo, cuando proceda y con carácter prioritario, la competencia basada en infraestructuras, reduciendo progresivamente la intervención *ex ante*

en los mercados, posibilitando la coinversión y el uso compartido y fomentando la innovación, teniendo debidamente en cuenta los riesgos en que incurren las empresas inversoras;

h) hacer posible el uso eficaz y eficiente de los recursos limitados de telecomunicaciones, como la numeración y el espectro radioeléctrico, la adecuada protección de este último, y el acceso a los derechos de ocupación de la propiedad pública y privada;

i) fomentar la neutralidad tecnológica en la regulación;

j) garantizar el cumplimiento de las obligaciones de servicio público en la explotación de redes y la prestación de servicios de comunicaciones electrónicas a las que se refiere el título III, en especial las de servicio universal;

k) defender los intereses de los usuarios, asegurando su derecho al acceso a los servicios de comunicaciones electrónicas en condiciones adecuadas de elección, precio y buena calidad, promoviendo la capacidad de los usuarios finales para acceder y distribuir la información o utilizar las aplicaciones y los servicios de su elección, en particular a través de un acceso abierto a internet. En la prestación de estos servicios deben salvaguardarse los imperativos constitucionales de no discriminación, de respeto a los derechos al honor y a la intimidad, la protección a la juventud y a la infancia, la protección a las personas con discapacidad, la protección de los datos personales y el secreto en las comunicaciones;

l) salvaguardar y proteger en los mercados de telecomunicaciones la satisfacción de las necesidades de grupos sociales específicos, las personas con discapacidad, las personas mayores, las personas en situación de dependencia y usuarios con necesidades sociales especiales, atendiendo a los principios de igualdad de oportunidades y no discriminación. En lo relativo al acceso a los servicios de comunicaciones electrónicas de las personas con discapacidad y personas en situación de dependencia, se fomentará el cumplimiento de las normas o las especificaciones pertinentes relativas a normalización técnica publicadas de acuerdo con la normativa comunitaria y se facilitará el acceso de los usuarios con discapacidad a los servicios de comunicaciones electrónicas y al uso de equipos terminales;

m) impulsar la universalización del acceso a las redes y servicios de comunicaciones electrónicas de banda ancha y contribuir a alcanzar la mayor vertebración territorial y social posible mediante el despliegue de redes y la prestación de servicios de comunicaciones electrónicas en las distintas zonas del territorio español, especialmente en aquellas que necesitan de la instalación de redes de comunicaciones electrónicas y la mejora de las existentes para permitir impulsar distintas actividades económicas y sociales.

Artículo 4. *Servicios de telecomunicaciones para la seguridad nacional, la defensa nacional, la seguridad pública, la seguridad vial y la protección civil.*

1. Sólo tienen la consideración de servicio público los servicios regulados en este artículo.

2. Las redes, servicios, instalaciones y equipos de telecomunicaciones que desarrollen actividades esenciales para la seguridad y defensa nacionales integran los medios destinados a éstas, se reservan al Estado y se rigen por su normativa específica.

3. El Ministerio de Asuntos Económicos y Transformación Digital es el órgano de la Administración General del Estado con competencia, de conformidad con la legislación específica sobre la materia y lo establecido en esta ley, para ejecutar, en la medida en que le afecte, la política de defensa nacional en el sector de las telecomunicaciones, con la debida coordinación con el Ministerio de Defensa y siguiendo los criterios fijados por éste.

En el marco de las funciones relacionadas con la defensa civil, corresponde al Ministerio de Asuntos Económicos y Transformación Digital estudiar, planear, programar, proponer y ejecutar cuantas medidas se relacionen con su aportación a la defensa nacional en el ámbito de las telecomunicaciones.

A tales efectos, los Ministerios de Defensa y de Asuntos Económicos y Transformación Digital coordinarán la planificación del sistema de telecomunicaciones de las Fuerzas Armadas, a fin de asegurar, en la medida de lo posible, su compatibilidad con los servicios civiles. Asimismo, elaborarán los programas de coordinación tecnológica precisos que faciliten la armonización, homologación y utilización, conjunta o indistinta, de los medios, sistemas y redes civiles y militares en el ámbito de las telecomunicaciones. Para el estudio e

informe de estas materias, se constituirán los órganos interministeriales que se consideren adecuados, con la composición y competencia que se determinen mediante real decreto.

4. En los ámbitos del orden público, la seguridad pública, seguridad vial y de la protección civil, en su específica relación con el uso de las telecomunicaciones, el Ministerio de Asuntos Económicos y Transformación Digital cooperará con el Ministerio del Interior y con los órganos responsables de las Comunidades Autónomas con competencias sobre las citadas materias.

5. Los bienes muebles o inmuebles vinculados a los centros, establecimientos y dependencias afectos a la instalación y explotación de las redes y a la prestación de los servicios de comunicaciones electrónicas dispondrán de las medidas y sistemas de seguridad, vigilancia, difusión de información, prevención de riesgos y protección que se determinen por el Gobierno, a propuesta de los Ministerios de Defensa, del Interior o de Asuntos Económicos y Transformación Digital, dentro del ámbito de sus respectivas competencias. Estas medidas y sistemas deberán estar disponibles en las situaciones de normalidad o en las de crisis, así como en los supuestos contemplados en la Ley Orgánica 4/1981, de 1 de junio, reguladora de los Estados de Alarma, Excepción y Sitio, la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la Protección de las Infraestructuras Críticas, la Ley 17/2015, de 9 de julio, del Sistema Nacional de Protección Civil y el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

6. El Gobierno, con carácter excepcional y transitorio, podrá acordar la asunción por la Administración General del Estado de la gestión directa de determinados servicios de comunicaciones electrónicas disponibles al público, distintos de los servicios de comunicaciones interpersonales, independientes de la numeración o de la explotación de ciertas redes públicas de comunicaciones electrónicas, para garantizar la seguridad pública y la seguridad nacional, en los términos en que dichas redes y servicios están definidos en el anexo II, excluyéndose en consecuencia las redes y servicios que se exploten o presten íntegramente en autoprestación. Esta facultad excepcional y transitoria de gestión directa podrá afectar a cualquier infraestructura, recurso asociado o elemento o nivel de la red o del servicio que resulte necesario para preservar o restablecer la seguridad pública y la seguridad nacional.

En ningún caso esta intervención podrá suponer una vulneración de los derechos fundamentales y libertades públicas reconocidas en el ordenamiento jurídico.

Asimismo, en el caso de incumplimiento de las obligaciones de servicio público a las que se refiere el título III, el Gobierno, previo informe preceptivo de la Comisión Nacional de los Mercados y la Competencia, e igualmente con carácter excepcional y transitorio, podrá acordar la asunción por la Administración General del Estado de la gestión directa de los correspondientes servicios o de la explotación de las correspondientes redes. En este último caso, podrá, con las mismas condiciones, intervenir la prestación de los servicios de comunicaciones electrónicas.

Los acuerdos de asunción de la gestión directa del servicio y de intervención de este o los de intervenir o explotar las redes a los que se refieren los párrafos anteriores se adoptarán por el Gobierno por propia iniciativa o a instancia de una Administración Pública competente. En este último caso, será preciso que la Administración Pública tenga competencias en materia de seguridad o para la prestación de los servicios públicos afectados por el anormal funcionamiento del servicio o de la red de comunicaciones electrónicas. En el supuesto de que el procedimiento se inicie a instancia de una Administración distinta de la del Estado, aquella tendrá la consideración de interesada y podrá evacuar informe con carácter previo a la resolución final.

Los acuerdos de asunción de la gestión directa del servicio y de intervención de este o los de intervenir o explotar las redes a los que se refiere este apartado deberán ser comunicados por el Gobierno en el plazo de veinticuatro horas al órgano jurisdiccional competente para que, en un plazo de cuarenta y ocho horas, establezca si los mismos resultan acordes con los derechos fundamentales y libertades públicas reconocidas en el ordenamiento jurídico, procediendo a su anulación en caso negativo.

7. La regulación contenida en esta ley se entiende sin perjuicio de lo previsto en la normativa específica sobre las telecomunicaciones relacionadas con el orden público, la seguridad pública, la defensa nacional y la seguridad nacional.

TÍTULO II

Suministro de redes y prestación de servicios de comunicaciones electrónicas en régimen de libre competencia

CAPÍTULO I

Disposiciones generales

Artículo 5. *Régimen de libre competencia.*

La instalación y explotación de las redes y la prestación de los servicios de comunicaciones electrónicas se realizará en régimen de libre competencia sin más limitaciones que las establecidas en esta ley y su normativa de desarrollo.

Artículo 6. *Requisitos exigibles para el suministro de las redes y la prestación de los servicios de comunicaciones electrónicas.*

1. Podrán suministrar redes públicas y prestar servicios de comunicaciones electrónicas disponibles al público las personas físicas o jurídicas nacionales de un Estado miembro de la Unión Europea o de un país perteneciente al Espacio Económico Europeo. Asimismo, podrán suministrar redes públicas y prestar servicios de comunicaciones electrónicas disponibles al público las personas físicas o jurídicas de otra nacionalidad, cuando así esté previsto en los acuerdos internacionales que vinculen al Reino de España, sin perjuicio de la aplicación de la normativa reguladora de las inversiones extranjeras. Para el resto de personas físicas o jurídicas, el Gobierno podrá autorizar excepciones de carácter general o particular a la regla anterior.

2. Los interesados en el suministro de una determinada red pública o en la prestación de un determinado servicio de comunicaciones electrónicas disponible al público deberán, con anterioridad al inicio de la actividad, notificarlo previamente al Registro de operadores previsto en el artículo 7, sometiéndose a las condiciones previstas para el ejercicio de la actividad que pretendan realizar. Esta obligación de notificación no resultará de aplicación a los interesados en la prestación de servicios de comunicaciones electrónicas interpersonales independientes de la numeración, así como para quienes suministren redes y presten servicios de comunicaciones electrónicas en régimen de autoprestación.

En la notificación se deberá proporcionar la siguiente información mínima:

a) nombre y apellidos o, en su caso, denominación o razón social y nacionalidad del operador;

b) datos de inscripción en el registro mercantil u otro registro público similar en el que figure el operador y número de identificación fiscal;

c) domicilio social y el señalado a los efectos de notificaciones;

d) el sitio web del proveedor, de haberlo, asociado al suministro de redes o servicios de comunicaciones electrónicas;

e) nombre, apellidos, número de documento nacional de identidad o pasaporte de su representante y de la persona responsable a los efectos de notificaciones, incluyendo, respecto a esta última la dirección de correo electrónico y número de teléfono móvil para poder recibir los avisos de puesta a disposición de las notificaciones que le sean enviadas;

f) una exposición sucinta de las redes y servicios que se propone suministrar;

g) una estimación de la fecha estimada de inicio de la actividad;

h) Estados miembros afectados.

3. Se regularán mediante real decreto los requisitos, la información a proporcionar y el procedimiento para efectuar las notificaciones a que se refiere el apartado anterior. En todo caso, cuando el Registro de operadores constate que las notificaciones no reúnen las

condiciones y requisitos establecidos dictará resolución motivada en un plazo máximo de quince días hábiles desde su presentación, no teniendo por realizadas aquéllas.

4. Los datos de las notificaciones contempladas en el apartado 2 que deban ser incluidos en la base de datos de la Unión Europea mencionada en el artículo 12 del Código Europeo de las Comunicaciones Electrónicas deberán ser puestos a disposición del Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (ORECE). La remisión de la citada información se realizará en los términos y plazos que se acuerden por el ORECE.

5. Cuando el suministro de acceso a una red pública de comunicaciones electrónicas a través de una red de área local radioeléctrica (RLAN) no forme parte de una actividad económica o sea accesorio respecto de otra actividad económica o un servicio público que no dependa del transporte de señales por esas redes, las empresas, las Administraciones públicas o usuarios finales que suministren el acceso no deberán efectuar la notificación a que se refiere el apartado 2 ni deberán inscribirse en el Registro de operadores.

6. Los interesados en la prestación de un determinado servicio de comunicaciones electrónicas interpersonales independientes de la numeración disponible al público deberán comunicarlo previamente al Registro de operadores, a efectos puramente estadísticos y censales.

7. Las Administraciones públicas comunicarán al Ministerio de Asuntos Económicos y Transformación Digital toda instalación o explotación de redes de comunicaciones electrónicas en régimen de autoprestación que haga uso del dominio público, tanto si dicha instalación o explotación se realiza de manera directa, a través de cualquier entidad o sociedad dependiente de ella o a través de cualquier entidad o sociedad a la que se le haya otorgado una concesión o habilitación al efecto.

El régimen de autoprestación en la instalación o explotación de dicha red puede ser total o parcial, y por tanto dicha comunicación deberá efectuarse aun cuando la capacidad excedentaria de la citada red pueda utilizarse para su explotación por terceros o para la prestación de servicios de comunicaciones electrónicas disponibles al público.

En el caso de que se utilice o esté previsto utilizar, directamente por la Administración Pública o por terceros, la capacidad excedentaria de estas redes de comunicaciones electrónicas en régimen de autoprestación, el Ministerio de Asuntos Económicos y Transformación Digital verificará el cumplimiento de lo previsto en el artículo 13. A tal efecto, la Administración Pública deberá proporcionar al Ministerio de Asuntos Económicos y Transformación Digital toda la información que le sea requerida a efecto de verificar dicho cumplimiento.

Mediante real decreto podrán especificarse aquellos supuestos en que, en atención a las características, la dimensión de la instalación o la naturaleza de los servicios a prestar, no resulte necesario que las Administraciones públicas efectúen la comunicación a que se refiere este apartado sobre la instalación de redes de comunicaciones electrónicas en régimen de autoprestación que haga uso del dominio público.

8. También deberá comunicarse al Ministerio de Asuntos Económicos y Transformación Digital la instalación o explotación de los puntos de intercambio de internet (IXP) ubicados en territorio español, a efecto de poder conocer y analizar la capacidad global de gestión y transmisión de todo el tráfico de comunicaciones electrónicas con origen, tránsito o destino en España.

9. Asimismo, deberá comunicarse al Ministerio de Asuntos Económicos y Transformación Digital la instalación o explotación de cables submarinos cuyo enganche, acceso o interconexión a redes de comunicaciones electrónicas se produzca en territorio español.

10. Mediante real decreto, que se aprobará en un plazo máximo de tres meses tras la publicación de la presente ley, se determinarán los datos que deberán aportarse y los plazos en los que efectuar las comunicaciones al Ministerio de Asuntos Económicos y Transformación Digital referidas en los apartados anteriores.

Artículo 7. *Registro de operadores.*

1. Se crea, dependiente de la Comisión Nacional de los Mercados y la Competencia, el Registro de operadores. Dicho Registro será de carácter público y su regulación se hará por real decreto. Se garantizará que el acceso a dicho Registro pueda efectuarse por medios electrónicos.

2. En el Registro deberán inscribirse los datos que se determinen mediante real decreto relativos a las personas físicas o jurídicas que hayan notificado, en los términos indicados en el apartado 2 del artículo 6, su intención de suministrar redes públicas o prestar servicios de comunicaciones electrónicas disponibles al público, las condiciones para desarrollar la actividad y sus modificaciones. Una vez realizada la notificación, el interesado adquirirá la condición de operador y podrá comenzar la prestación del servicio o el suministro de la red, sin perjuicio de lo dispuesto en el artículo 6.3.

3. A petición del operador inscrito, el Registro de operadores emitirá, en el plazo de una semana desde la presentación de dicha petición, una declaración normalizada que confirme que ha presentado la notificación la persona interesada en el suministro de una determinada red pública o en la prestación de un determinado servicio de comunicaciones electrónicas disponible al público. Dicha declaración detallará las circunstancias en que los operadores tienen derecho a solicitar derechos de suministro de redes y recursos, negociar la interconexión y obtener el acceso o la interconexión para así facilitar el ejercicio de estos derechos.

4. Quienes resultasen seleccionados para la prestación de servicios de comunicaciones electrónicas armonizados en procedimientos de licitación convocados por las instituciones de la Unión Europea serán inscritos de oficio en el Registro de operadores.

5. No será preciso el consentimiento del interesado para el tratamiento de los datos de carácter personal que haya de contener el Registro ni para la comunicación de dichos datos que se derive de su publicidad.

Artículo 8. *Condiciones para el suministro de redes y prestación de servicios de comunicaciones electrónicas.*

1. El suministro de redes y la prestación de los servicios de comunicaciones electrónicas se sujetarán a las condiciones previstas en esta ley y su normativa de desarrollo, entre las cuales se incluirán las de salvaguarda de los derechos de los usuarios finales.

2. La adquisición de los derechos de uso del dominio público radioeléctrico, de ocupación del dominio público o de la propiedad privada y de los recursos de numeración necesarios para la instalación y explotación de redes y para la prestación de servicios de comunicaciones electrónicas deberá realizarse conforme a lo dispuesto en esta ley y en lo no contemplado en la misma por su normativa específica.

Artículo 9. *Obligaciones de suministro de información.*

1. El Ministerio de Asuntos Económicos y Transformación Digital y la Comisión Nacional de los Mercados y la Competencia podrán, en el ámbito de su actuación, requerir a las personas físicas o jurídicas que suministren redes o presten servicios de comunicaciones electrónicas, recursos asociados, servicios asociados e infraestructuras digitales, incluyendo los puntos de intercambio de internet (IXP) y centros de proceso de datos (CPD), en especial en éstos últimos, los que estén directamente vinculados al suministro de redes o a la prestación de servicios de comunicaciones electrónicas, así como a aquellos otros agentes que intervengan en este mercado o en mercados y sectores estrechamente relacionados, incluyendo los proveedores de contenidos y de servicios digitales, la información necesaria, incluso financiera, para el cumplimiento de alguna de las siguientes finalidades:

a) satisfacer necesidades estadísticas o de análisis y para la elaboración de estudios e informes de seguimiento sectoriales;

b) comprobar el cumplimiento de las condiciones establecidas para la prestación de servicios o el suministro de redes de comunicaciones electrónicas, en particular, cuando la explotación de las redes conlleve emisiones radioeléctricas;

c) comprobar que la prestación de servicios o el suministro de redes de comunicaciones electrónicas por parte de operadores controlados directa o indirectamente por Administraciones públicas cumplen las condiciones establecidas por esta ley y sus normas de desarrollo;

d) evaluar la procedencia de las solicitudes de derechos de uso del dominio público radioeléctrico y de la numeración;

e) comprobar el uso efectivo y eficiente de frecuencias y números y el cumplimiento de las obligaciones que resulten de los derechos de uso del dominio público radioeléctrico, de la numeración o de la ocupación del dominio público o de la propiedad privada;

f) elaborar análisis que permitan la definición de los mercados de referencia, el establecimiento de condiciones específicas a los operadores con peso significativo de mercado en aquéllos y conocer el modo en que la futura evolución de las redes o los servicios puede repercutir en los servicios mayoristas que las empresas ponen a disposición de sus competidores. Asimismo, podrá exigirse a las empresas con un peso significativo en los mercados mayoristas que presenten datos sobre los mercados descendentes o minoristas asociados con dichos mercados mayoristas, incluyendo datos contables, así como sobre otros mercados estrechamente relacionados;

g) comprobar el cumplimiento de las obligaciones específicas impuestas en el marco de la regulación *ex ante* y el cumplimiento de las resoluciones dictadas para resolver conflictos entre operadores;

h) comprobar el cumplimiento de las obligaciones de servicio público y obligaciones de carácter público, así como determinar los operadores encargados de prestar el servicio universal;

i) comprobar el cumplimiento de las obligaciones que resulten necesarias para garantizar un acceso equivalente para los usuarios finales con discapacidad y que éstos se beneficien de la posibilidad de elección de empresas y servicios disponibles para la mayoría de los usuarios finales;

j) la puesta a disposición de los ciudadanos de información o aplicaciones interactivas que posibiliten realizar comparativas sobre precios, cobertura y calidad de los servicios, en interés de los usuarios;

k) la adopción de medidas destinadas a facilitar la coubicación o el uso compartido de elementos de redes públicas de comunicaciones electrónicas y recursos asociados;

l) evaluar la integridad y la seguridad de las redes y servicios de comunicaciones electrónicas;

m) planificar de manera eficiente el uso de fondos públicos destinados, en su caso, al despliegue de infraestructuras de telecomunicaciones;

n) evaluar la futura evolución de la red o del servicio que pueda tener repercusiones sobre los servicios al por mayor puestos a disposición de la competencia, sobre la cobertura territorial, la conectividad a disposición de los usuarios finales o en la determinación de zonas para el uso de fondos públicos destinados al despliegue de infraestructuras de telecomunicaciones;

ñ) efectuar estudios geográficos;

o) cumplir los requerimientos que vengan impuestos en el ordenamiento jurídico, incluyendo la información que pueda resultar necesaria para responder a solicitudes motivadas de información del ORECE y de la Comisión Europea;

p) comprobar el cumplimiento del resto de obligaciones establecidas en esta ley y su normativa de desarrollo, así como en la normativa comunitaria.

La información a la que se refiere este apartado, excepto aquella a la que se refieren las letras d) y m), no podrá exigirse antes del inicio de la actividad y se suministrará en el plazo y forma que se establezca en cada requerimiento, atendidas las circunstancias del caso.

2. Las Administraciones públicas podrán solicitar la información que sea necesaria en el ejercicio de sus competencias.

Las Administraciones públicas, antes de solicitar información en materia de telecomunicaciones a las personas físicas o jurídicas que suministren redes o presten servicios de comunicaciones electrónicas para el ejercicio de sus funciones, deberán recabar dicha información del Ministerio de Asuntos Económicos y Transformación Digital o de la Comisión Nacional de los Mercados y la Competencia. Únicamente en el caso de que estas autoridades no dispongan de la información solicitada o la misma no pueda ser proporcionada al ser confidencial por razones de seguridad o de secreto comercial o industrial, los órganos competentes de las Administraciones públicas podrán solicitar dicha información en materia de telecomunicaciones de las personas físicas o jurídicas que suministren redes o presten servicios de comunicaciones electrónicas.

3. La Comisión Nacional de los Mercados y la Competencia podrá solicitar información del punto de información único establecido de acuerdo al Real Decreto 330/2016, de 9 de septiembre, relativo a medidas para reducir el coste del despliegue de las redes de comunicaciones electrónicas de alta velocidad.

4. Las solicitudes de información que se realicen de conformidad con los apartados anteriores habrán de ser motivadas, proporcionadas al fin perseguido y se indicarán los fines concretos para los que va a utilizarse dicha información.

5. En todo caso, se garantizará la confidencialidad de la información suministrada que pueda afectar a la seguridad e integridad de las redes y de los servicios de comunicaciones electrónicas o al secreto comercial o industrial.

Artículo 10. *Normas técnicas.*

1. El Ministerio de Asuntos Económicos y Transformación Digital garantizará la utilización de las normas o especificaciones técnicas cuya aplicación declare obligatoria la Comisión Europea, de conformidad con lo establecido en la normativa de la Unión Europea.

Asimismo, el Ministerio de Asuntos Económicos y Transformación Digital fomentará el uso de las normas o especificaciones técnicas identificadas en la relación que la Comisión Europea elabore como base para fomentar la armonización del suministro de redes de comunicaciones electrónicas, servicios de comunicaciones electrónicas y recursos y servicios asociados, en la medida estrictamente necesaria para garantizar la interoperabilidad de los servicios y la conectividad de extremo a extremo, la facilitación del cambio de proveedor y la conservación de la numeración, y para mejorar la libertad de elección de los usuarios.

En ausencia de normas o especificaciones técnicas identificadas por la Comisión Europea para fomentar la armonización, se promoverá la aplicación de las normas o especificaciones aprobadas por los organismos europeos de normalización.

A su vez, en ausencia de dichas normas o especificaciones, el Ministerio de Asuntos Económicos y Transformación Digital promoverá la aplicación de las normas o recomendaciones internacionales aprobadas por la Unión Internacional de Telecomunicaciones (UIT), la Conferencia Europea de Administraciones de Correos y Telecomunicaciones (CEPT), el Instituto Europeo de Normas de Telecomunicaciones (ETSI), el Comité Europeo de Normalización (CEN), el Comité Europeo de Normalización Electrotécnica (CENELEC), la Comisión Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (CEI).

Mediante real decreto se podrán determinar las formas de elaboración y, en su caso, de adopción de las especificaciones técnicas aplicables a redes y servicios de comunicaciones electrónicas, en particular, a efectos de garantizar el cumplimiento de requisitos en materia de despliegue de redes, obligaciones de servicio público, interoperabilidad, integridad y seguridad de redes y servicios.

Mediante real decreto se establecerá el procedimiento de comunicación de las citadas especificaciones a la Comisión Europea de conformidad con la normativa de la Unión Europea.

2. La Comisión Nacional de los Mercados y la Competencia también fomentará y garantizará el uso de las normas o especificaciones técnicas en los términos señalados en el apartado anterior en el ejercicio de sus funciones.

CAPÍTULO II

Notificaciones

Artículo 11. *Derechos derivados de la notificación.*

1. La notificación a que se refiere el artículo 6.2 habilita a ejercer los derechos establecidos en esta ley y su normativa de desarrollo.

2. En particular, la notificación habilita a la siguiente lista mínima de derechos:

a) suministrar redes y prestar servicios de comunicaciones electrónicas;

b) poder obtener derechos de uso y ocupación de propiedad privada y de dominio público en los términos indicados en el título III;

c) poder obtener derechos de uso de dominio público radioeléctrico en los términos indicados en el título V;

d) poder obtener derechos de uso de los recursos de numeración, en los términos indicados en el capítulo VII;

e) negociar la interconexión y, en su caso, obtener el acceso o la interconexión a partir de otros proveedores de redes públicas de comunicaciones electrónicas o de servicios de comunicaciones electrónicas disponibles al público habilitados;

f) tener oportunidad de ser designados para suministrar diferentes elementos de servicio universal de telecomunicaciones o cubrir diferentes partes del territorio nacional;

g) poder resultar seleccionados para el suministro de redes y la prestación de servicios de comunicaciones electrónicas en procedimientos de licitación convocados por las Administraciones públicas.

Artículo 12. *Obligaciones derivadas de la notificación.*

1. La notificación a que se refiere el artículo 6.2 obliga a cumplir con las cargas y obligaciones establecidas en esta ley y su normativa de desarrollo.

2. Las obligaciones específicas que se impongan en materia de acceso e interconexión en virtud de lo dispuesto en el título II y las que se impongan en la prestación del servicio universal de telecomunicaciones a tenor de lo establecido en el título III son jurídicamente independientes de los derechos y obligaciones que se derivan de la notificación a que se refiere el artículo 6.2.

3. Los operadores que, de acuerdo con la legislación vigente, tengan derechos especiales o exclusivos para la prestación de servicios en otro sector económico y que exploten redes públicas o presten servicios de comunicaciones electrónicas disponibles al público deberán llevar cuentas separadas y auditadas para sus actividades de comunicaciones electrónicas, o establecer una separación estructural efectiva para las actividades asociadas con la explotación de redes o la prestación de servicios de comunicaciones electrónicas. Mediante real decreto podrá establecerse la exención de esta obligación para las entidades cuyos ingresos brutos de explotación anuales por actividades asociadas con las redes o servicios de comunicaciones electrónicas sea inferior a 50 millones de euros en la Unión Europea.

Artículo 13. *Suministro de redes públicas y prestación de servicios de comunicaciones electrónicas en régimen de prestación a terceros por las Administraciones públicas.*

1. La instalación y explotación de redes públicas o la prestación de servicios de comunicaciones electrónicas disponibles al público por operadores controlados directa o indirectamente por Administraciones públicas se regirá de manera específica por lo dispuesto en el presente artículo. En su actuación, las Administraciones públicas deberán velar por el cumplimiento de los principios generales contemplados en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, incluyendo en particular los principios de eficacia, de economía, suficiencia y adecuación estricta de los medios a los fines institucionales, y de eficiencia en la asignación y utilización de los recursos públicos.

2. La instalación y explotación de redes públicas o la prestación de servicios de comunicaciones electrónicas disponibles al público por operadores controlados directa o indirectamente por Administraciones públicas se realizará dando cumplimiento al principio de inversor privado, con la debida separación de cuentas, con arreglo a los principios de neutralidad, transparencia, no distorsión de la competencia y no discriminación, y cumpliendo con la normativa sobre ayudas de Estado a que se refieren los artículos 107 y 108 del Tratado de Funcionamiento de la Unión Europea.

Mediante real decreto, previo informe de la Comisión Nacional de los Mercados y la Competencia, se determinarán las condiciones en que los operadores controlados directa o indirectamente por Administraciones públicas deberán llevar a cabo la instalación y explotación de redes públicas o la prestación de servicios de comunicaciones electrónicas disponibles al público y, en especial, los criterios, condiciones y requisitos para que dichos operadores actúen con sujeción al principio de inversor privado en una economía de

mercado. En particular, en dicho real decreto se establecerán los supuestos en los que, como excepción a la exigencia de actuación con sujeción al principio de inversor privado en una economía de mercado, los operadores controlados directa o indirectamente por Administraciones públicas podrán instalar, desplegar y explotar redes públicas y prestar servicios de comunicaciones electrónicas disponibles al público que no distorsionen la competencia o cuando se confirme fallo del mercado y no exista interés de concurrencia en el despliegue del sector privado por ausencia o insuficiencia de inversión privada, ajustándose la inversión pública al principio de necesidad, con la finalidad de garantizar la necesaria cohesión territorial y social.

En las iniciativas llevadas a cabo por los órganos competentes de las Administraciones públicas y entidades dependientes de ellas para la difusión a los ciudadanos del servicio de televisión digital en zonas donde no exista cobertura del servicio de televisión digital terrestre, se considera que se produce una situación de fallo de mercado. Por ello, estas iniciativas no deben sujetarse al principio de inversor privado ni deben comunicarse al Registro de operadores, salvo que la red de comunicaciones electrónicas que sirva de soporte para efectuar la difusión del servicio de televisión digital en zonas donde no exista cobertura del servicio de televisión digital terrestre se ponga a disposición de terceros, a título oneroso o gratuito, o que a través de la misma se presten otros servicios disponibles al público distintos del mencionado servicio de televisión digital, en cuyo caso se deberá cumplir lo establecido en este artículo.

3. Una Administración Pública podrá instalar, desplegar y explotar redes públicas de comunicaciones electrónicas o prestar servicios de comunicaciones disponibles al público directamente o a través de entidades o sociedades que tengan entre su objeto social o finalidad la instalación y explotación de redes o la prestación de servicios de comunicaciones electrónicas.

La instalación o explotación de redes públicas de comunicaciones electrónicas y la prestación de servicios de comunicaciones electrónicas disponibles al público por los órganos o entes gestores de infraestructuras de transporte de competencia estatal, se realizará en las condiciones establecidas en el artículo 54.

4. La instalación y explotación de redes públicas o la prestación de servicios de comunicaciones electrónicas disponibles al público por operadores controlados directa o indirectamente por Administraciones públicas deberán llevarse a cabo en las condiciones establecidas en el artículo 8 y, en particular, en las siguientes condiciones:

a) los operadores tienen reconocido directamente el derecho a acceder en condiciones neutrales, objetivas, transparentes, equitativas y no discriminatorias a las infraestructuras y recursos asociados utilizados por los operadores controlados directa o indirectamente por Administraciones públicas para la instalación y explotación de redes de comunicaciones electrónicas;

b) los operadores tienen reconocido directamente el derecho de uso compartido de las infraestructuras de red de comunicaciones electrónicas y sus recursos asociados instaladas por los operadores controlados directa o indirectamente por Administraciones públicas en condiciones neutrales, objetivas, transparentes, equitativas y no discriminatorias;

c) si las Administraciones públicas reguladoras o titulares del dominio público ostentan la propiedad, total o parcial, o ejercen el control directo o indirecto de operadores que explotan redes públicas de comunicaciones electrónicas o servicios de comunicaciones electrónicas disponibles para el público, deberán mantener una separación estructural entre dichos operadores y los órganos encargados de la regulación y gestión de los derechos de utilización del dominio público correspondiente.

5. Se permite a las Administraciones públicas el suministro al público de acceso a RLAN, sin ajustarse a los requisitos establecidos en el apartado 3:

a) cuando dicho suministro es accesorio respecto de los servicios públicos suministrados en los locales ocupados por las Administraciones públicas o en espacios públicos cercanos a estos locales, que se determinen reglamentariamente.

b) cuando se desarrollen iniciativas que agregan y permiten el acceso recíproco o de otra forma a sus RLAN por parte de diferentes usuarios finales.

c) cuando el suministro de acceso a una red pública de comunicaciones electrónicas a través de una RLAN no forme parte de una actividad económica o sea accesorio respecto de otra actividad económica o un servicio público que no dependa del transporte de señales por esas redes, las Administraciones públicas que suministren el acceso no deberán efectuar la notificación a que se refiere el artículo 6.2 ni deberán inscribirse en el Registro de operadores.

6. La instalación y explotación de redes públicas o la prestación de servicios de comunicaciones electrónicas disponibles al público por parte de Administraciones públicas que se lleve a cabo en el marco de programas de ayudas otorgadas directamente por la Comisión Europea y sus Servicios o entidades se regirá en exclusiva por el instrumento que regule el otorgamiento de las ayudas y el resto de normativa europea, no siendo necesaria la inscripción de la Administración Pública en el Registro de operadores.

CAPÍTULO III

Acceso a las redes y recursos asociados e interconexión

Artículo 14. *Principios generales aplicables al acceso a las redes y recursos asociados y a su interconexión.*

1. Este capítulo y su desarrollo reglamentario serán aplicables a la interconexión y a los accesos a redes públicas de comunicaciones electrónicas y a sus recursos asociados, salvo que el beneficiario del acceso sea un usuario final, de acuerdo con la definición que se da a los conceptos de acceso e interconexión en el anexo II.

2. Los operadores de redes públicas de comunicaciones electrónicas tendrán el derecho y, cuando se solicite por otros operadores de redes de comunicaciones electrónicas, la obligación de negociar la interconexión mutua con el fin de prestar servicios de comunicaciones electrónicas disponibles al público, con el objeto de garantizar así la prestación de servicios y su interoperabilidad.

Las empresas, autoridades públicas o usuarios finales que suministren el acceso a una red pública de comunicaciones electrónicas a través de RLAN, cuando dicho suministro no forme parte de una actividad económica o sea accesorio respecto de otra actividad económica o un servicio público que no dependa del transporte de señales por esas redes, no estarán sujetos a la obligación de interconectar su red RLAN.

3. No existirán restricciones que impidan que los operadores negocien entre sí acuerdos de acceso e interconexión.

4. La persona física o jurídica habilitada para suministrar redes o prestar servicios en otro Estado miembro de la Unión Europea que solicite acceso o interconexión en España no necesitará llevar a cabo la notificación a la que se refiere el artículo 6.2 cuando no suministre redes ni preste servicios de comunicaciones electrónicas en el territorio nacional.

5. El Ministerio de Asuntos Económicos y Transformación Digital y la Comisión Nacional de los Mercados y la Competencia fomentarán y, cuando sea pertinente, garantizarán, de conformidad con lo dispuesto en la presente ley y su normativa de desarrollo, la adecuación del acceso, la interconexión y la interoperabilidad de los servicios, y ejercerán sus responsabilidades de tal modo que se promueva la eficiencia, la competencia sostenible, el despliegue de redes de muy alta capacidad, la innovación e inversión eficientes y el máximo beneficio para los usuarios finales.

6. En particular, el Ministerio de Asuntos Económicos y Transformación Digital podrá imponer:

a) en casos justificados y en la medida en que sea necesario, obligaciones a los operadores que controlen el acceso a los usuarios finales para que sus servicios sean interoperables;

b) en casos justificados, cuando la conectividad de extremo a extremo entre usuarios finales esté en peligro debido a una falta de interoperabilidad entre los servicios de comunicaciones interpersonales, y en la medida en que sea necesario para garantizar la conectividad de extremo a extremo entre usuarios finales, obligaciones a los proveedores de servicios de comunicaciones interpersonales independientes de la numeración para que sus

servicios sean interoperables. Estas obligaciones únicamente podrán imponerse cuando se den las dos circunstancias siguientes:

1.º en la medida necesaria para garantizar la interoperabilidad de los servicios de comunicaciones interpersonales, y podrán incluir, para los proveedores de dichos servicios, obligaciones proporcionadas de publicar y autorizar la utilización, modificación y redistribución de información pertinente por parte de las autoridades y de otros proveedores, o la obligación de utilizar o aplicar normas de armonización o cualesquiera otras normas europeas o internacionales pertinentes;

2.º cuando la Comisión Europea, previa consulta al ORECE y teniendo especialmente en cuenta su dictamen, haya encontrado una amenaza considerable para la conectividad de extremo a extremo entre los usuarios finales y haya adoptado medidas de ejecución para especificar la naturaleza y el alcance de cualesquiera obligaciones que puedan imponerse.

7. A su vez, y sin perjuicio de las medidas que puedan adoptarse en relación con las empresas que tengan un peso significativo en el mercado de acuerdo con lo previsto en el artículo 18, la Comisión Nacional de los Mercados y la Competencia podrá imponer:

a) en la medida en que sea necesario garantizar la posibilidad de conexión de extremo a extremo, obligaciones a operadores que controlen el acceso a los usuarios finales, incluida, en casos justificados, la obligación de interconectar sus redes cuando no lo hayan hecho;

b) en la medida en que sea necesario para garantizar el acceso de los usuarios finales a los servicios digitales de comunicación audiovisual televisivo o radiofónico y los servicios complementarios conexos, obligaciones a los operadores para que faciliten acceso a los interfaces de programa de aplicaciones (API) y guías electrónicas de programación (EPG), en condiciones justas, razonables y no discriminatorias.

8. Las obligaciones y condiciones que se impongan de conformidad con este capítulo serán objetivas, transparentes, proporcionadas y no discriminatorias.

9. Los operadores que obtengan información de otros, con anterioridad, durante o con posterioridad al proceso de negociación de acuerdos de acceso o interconexión, destinarán dicha información exclusivamente a los fines para los que les fue facilitada y respetarán en todo momento la confidencialidad de la información transmitida o almacenada, en especial respecto de terceros, incluidos otros departamentos de la propia empresa, filiales o asociados.

CAPÍTULO IV

Regulación *ex ante* de los mercados

Artículo 15. *Definición de mercados de referencia.*

1. La Comisión Nacional de los Mercados y la Competencia, teniendo en cuenta la Recomendación de la Comisión Europea sobre mercados relevantes de productos y servicios, las Directrices de la Comisión Europea para el análisis del mercado y evaluación del peso significativo en el mercado y los dictámenes y posiciones comunes pertinentes adoptados por el Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (ORECE), definirá, previo informe de la Secretaría de Estado de Economía y Apoyo a la Empresa y de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales y mediante resolución publicada en el «Boletín Oficial del Estado», los mercados de referencia relativos a redes y servicios de comunicaciones electrónicas, entre los que se incluirán los correspondientes mercados de referencia, y el ámbito geográfico de los mismos, cuyas características pueden justificar la imposición de obligaciones específicas. A tal efecto, tendrá en cuenta los resultados del estudio geográfico a que se refiere el artículo 48.

2. La Comisión Nacional de los Mercados y la Competencia podrá presentar junto con la autoridad nacional de reglamentación de otro u otros Estados miembros una solicitud motivada al ORECE, a fin de que este organismo efectúe un análisis relativo a la posible existencia de un mercado transnacional, para su posterior valoración por la Comisión Europea. En el caso de mercados transnacionales determinados por la Comisión Europea, las autoridades nacionales de reglamentación afectadas efectuarán un análisis conjunto de

mercado y se pronunciarán concertadamente sobre la imposición, el mantenimiento, la modificación o la supresión de las obligaciones específicas.

3. La Comisión Nacional de los Mercados y la Competencia, junto con la autoridad nacional de reglamentación de otro u otros Estados miembros, también podrán notificar conjuntamente sus proyectos de medidas en relación con el análisis del mercado y cualesquiera obligaciones reglamentarias en ausencia de mercados transnacionales, cuando consideren que las condiciones de mercado en sus respectivas jurisdicciones son suficientemente homogéneas.

4. En todo caso, la Comisión Nacional de los Mercados y la Competencia, en aplicación de la normativa en materia de competencia, en especial, de la Ley 15/2007, de 3 de julio, de Defensa de la Competencia, de los artículos 101 y 102 del Tratado de Funcionamiento de la Unión Europea, y de la Ley 3/2013, de 4 de junio, de creación de la Comisión Nacional de los Mercados y la Competencia, deberá supervisar el funcionamiento de los distintos mercados de comunicaciones electrónicas, así como la actividad de los operadores ya tengan o no peso significativo en el mercado, para preservar, garantizar y promover condiciones de competencia efectiva en los mismos.

Artículo 16. *Análisis de los mercados de referencia.*

1. Teniendo en cuenta las referencias citadas en el artículo 15, la Comisión Nacional de los Mercados y la Competencia llevará a cabo un análisis de los citados mercados:

a) En un plazo máximo de cinco años contado desde la adopción de una medida anterior cuando la Comisión Nacional de los Mercados y la Competencia haya definido el mercado pertinente y determinado qué operadores tienen un peso significativo en el mercado.

Con carácter excepcional dicho plazo podrá ampliarse hasta un año adicional previa notificación a la Comisión Europea cuatro meses antes de que expire el plazo inicial de cinco años y sin que ésta haya manifestado objeción alguna en un mes desde la fecha de tal notificación.

En caso de mercados dinámicos, deberá realizarse un análisis del mercado cada tres años. Los mercados deben ser considerados como dinámicos si la evolución tecnológica y las pautas de demanda de los usuarios finales pueden evolucionar de manera tal que las conclusiones del análisis quedarían superadas a medio plazo en un grupo significativo de zonas geográficas o de usuarios finales dentro del mercado geográfico y de producto que defina la Comisión Nacional de los Mercados y la Competencia.

b) En el plazo máximo de tres años desde la adopción de una recomendación revisada sobre mercados pertinentes, para los mercados no notificados previamente a la Comisión Europea.

2. Si la Comisión Nacional de los Mercados y la Competencia considera que no puede concluir o no hubiera concluido su análisis de un mercado relevante que figura en la Recomendación de mercados relevantes dentro de los plazos establecidos, el ORECE le prestará asistencia, a petición de la propia Comisión, para la conclusión del análisis del mercado concreto y la determinación de las obligaciones específicas que deban imponerse. La Comisión Nacional de los Mercados y la Competencia, contando con esta colaboración, notificará el proyecto de medida a la Comisión Europea en un plazo de seis meses.

3. El Ministerio de Asuntos Económicos y Transformación Digital, en virtud de lo dispuesto en el artículo 5.2 de la Ley 3/2013, de 4 de junio, de creación de la Comisión Nacional de los Mercados y la Competencia, podrá solicitar a la Comisión Nacional de los Mercados y la Competencia para que realice el análisis de un mercado determinado de comunicaciones electrónicas cuando concurran razones de interés general, las condiciones competitivas de dicho mercado se hayan modificado sustancialmente o bien se aprecien indicios de falta de competencia efectiva.

4. La Comisión Nacional de los Mercados y la Competencia, en los planes anuales o plurianuales de actuación que apruebe y en los que debe constar sus objetivos y prioridades a tenor de lo dispuesto en el artículo 20.16 de la Ley 3/2013, de 4 de junio, de creación de la Comisión Nacional de los Mercados y la Competencia, deberá identificar los mercados relevantes que vaya a analizar y las actuaciones necesarias para la adecuada realización de dicho análisis dentro de los plazos previstos en este artículo.

5. La persona titular de la Presidencia de la Comisión Nacional de los Mercados y la Competencia, en el marco del control parlamentario anual a que se refiere el artículo 39.1 de la Ley 3/2013, de 4 de junio, de creación de la Comisión Nacional de los Mercados y la Competencia, deberá dar cuenta del resultado de los análisis de los mercados y el cumplimiento de los plazos establecidos en este artículo.

Artículo 17. *Procedimiento para la imposición de obligaciones específicas.*

1. La Comisión Nacional de los Mercados y la Competencia, previo informe de la Secretaría de Estado de Economía y Apoyo a la Empresa y de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, determinará si en un mercado considerado se justifica la imposición de las obligaciones específicas apropiadas.

Puede considerarse que en un mercado considerado se justifica la imposición de las obligaciones específicas si se cumplen todos los criterios siguientes:

a) la presencia de barreras de entrada, importantes y no transitorias, de tipo estructural, jurídico o reglamentario;

b) la existencia de una estructura del mercado que no tiende hacia una competencia efectiva dentro del horizonte temporal pertinente, teniendo en cuenta el grado de competencia basada en la infraestructura y de otras fuentes de competencia detrás de las barreras de entrada;

c) el hecho de que la legislación en materia de competencia por sí sola resulte insuficiente para abordar adecuadamente las deficiencias del mercado detectadas.

2. Cuando la Comisión Nacional de los Mercados y la Competencia realice un análisis de un mercado incluido en la Recomendación de la Comisión Europea sobre mercados relevantes de productos y servicios, considerará que concurren los criterios establecidos en las letras a), b) y c) del apartado anterior, a menos que, a la vista de las circunstancias nacionales específicas, determine que uno o varios de dichos criterios no se cumplen.

3. A la hora de analizar si se justifica la imposición de las obligaciones específicas en un mercado considerado, la Comisión Nacional de los Mercados y la Competencia considerará la evolución desde una perspectiva de futuro en ausencia de regulación impuesta en dicho mercado pertinente, teniendo en cuenta:

a) la evolución del mercado que afecte a la probabilidad de que el mercado pertinente tienda hacia la competencia efectiva;

b) todas las restricciones competitivas pertinentes, a nivel mayorista y minorista, con independencia de que las causas de dichas restricciones se consideren redes de comunicaciones electrónicas, servicios de comunicaciones electrónicas u otros tipos de servicios o aplicaciones que sean comparables desde la perspectiva del usuario final, y con independencia de que dichas restricciones formen parte del mercado pertinente;

c) otros tipos de reglamentación o medidas impuestas que afecten al mercado pertinente o al mercado o mercados minoristas conexos durante el período pertinente, y

d) la regulación impuesta a otros mercados pertinentes.

4. La Comisión Nacional de los Mercados y la Competencia, una vez determinado si en un mercado considerado se justifica la imposición de las obligaciones específicas, podrá, previo informe de la Secretaría de Estado de Economía y Apoyo a la Empresa y de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, imponer obligaciones específicas o mantener o modificar obligaciones específicas que tuvieran impuestas.

En los mercados en los que se llegue a la conclusión de que no se justifica la imposición de las obligaciones específicas, la Comisión Nacional de los Mercados y la Competencia no impondrá o mantendrá obligaciones específicas y suprimirá las obligaciones específicas impuestas.

5. Cuando la Comisión Nacional de los Mercados y la Competencia determine que en un mercado considerado se justifica la imposición de las obligaciones específicas, determinará, identificará y hará públicos, previo informe de la Secretaría de Estado de Economía y Apoyo a la Empresa y de la Secretaría de Estado de Telecomunicaciones e Infraestructuras

Digitales, el operador u operadores que, individual o conjuntamente, poseen un peso significativo en cada mercado considerado.

Cuando un operador tenga un peso significativo en un mercado determinado, la Comisión Nacional de los Mercados y la Competencia podrá considerar que tiene también un peso significativo en un mercado estrechamente relacionado con aquel si los vínculos entre los dos mercados son tales que, gracias al efecto de apalancamiento, resulta posible ejercer en el mercado estrechamente relacionado el peso que se tiene en el mercado determinado, reforzando así el peso del operador en el mercado. En este supuesto, podrán imponerse obligaciones específicas adecuadas en el mercado estrechamente relacionado, en virtud del artículo 18.

Artículo 18. *Obligaciones específicas aplicables a los operadores con peso significativo en mercados de referencia.*

1. La Comisión Nacional de los Mercados y la Competencia, en la forma y en las condiciones que se determinen en desarrollo de lo dispuesto en el apartado 8 de este artículo, podrá imponer a los operadores que hayan sido declarados con peso significativo en el mercado obligaciones específicas en materia de:

a) transparencia, en relación con la interconexión y el acceso, conforme a las cuales los operadores deberán hacer público determinado tipo de información, como la relativa a la contabilidad, los precios, las especificaciones técnicas, las características de las redes y su evolución probable, las condiciones de suministro y utilización, incluidas todas las condiciones que modifiquen el acceso o la utilización de los servicios y aplicaciones, en especial en relación con la migración desde una infraestructura heredada.

En particular, cuando de conformidad con la letra b) de este apartado se impongan a un operador obligaciones de no discriminación, se le podrá exigir que publique una oferta de referencia, que deberá estar suficientemente desglosada para garantizar que no se exija a los operadores pagar por recursos que sean innecesarios para el servicio requerido. Dicha oferta contendrá las ofertas pertinentes subdivididas por componentes de acuerdo con las necesidades del mercado, así como las condiciones correspondientes, incluidos los precios. La Comisión Nacional de los Mercados y la Competencia podrá determinar la información concreta a incluir e imponer cambios en las ofertas de referencia, para hacer efectivas las obligaciones a que se refiere este capítulo.

Asimismo, se garantizará que los operadores a los que de conformidad con las letras d) y e) se impongan obligaciones en relación con el acceso al por mayor a la infraestructura de la red dispongan y publiquen una oferta de referencia, debiendo especificar unos indicadores de rendimiento clave, en su caso, así como los niveles de servicio correspondientes;

b) no discriminación en relación con la interconexión y el acceso, que garantizarán, en particular, que el operador aplique condiciones equivalentes en circunstancias semejantes a otros operadores que presten servicios equivalentes y proporcione a terceros servicios e información de la misma calidad que los que proporcione para sus propios servicios o los de sus filiales o asociados y en las mismas condiciones.

La Comisión Nacional de los Mercados y la Competencia podrá imponer al operador con peso significativo en el mercado obligaciones de suministrar productos y servicios de acceso a todos los operadores, incluido él mismo, en los mismos plazos, términos y condiciones, incluso en lo relacionado con niveles de precios y servicios, y a través de los mismos sistemas y procesos, con el fin de garantizar la equivalencia de acceso;

c) separación de cuentas, en el formato y con la metodología que, en su caso, se especifiquen.

En particular, se podrá exigir a un operador integrado verticalmente que ponga de manifiesto de manera transparente los precios al por mayor y los precios de transferencia internos que practica, para garantizar el cumplimiento de una obligación de no discriminación o, cuando proceda, para impedir las subvenciones cruzadas de carácter desleal;

d) acceso a la obra civil, al efecto de satisfacer las solicitudes razonables de acceso y de uso de obra civil, incluidos, entre otros, edificios o accesos a edificios, cableado, antenas, torres y otras estructuras de soporte, postes, mástiles, conductos, tuberías, cámaras de inspección, bocas de inspección y armarios, en situaciones en las que se llegue a la

conclusión de que la denegación de acceso o el acceso otorgado en virtud de términos y condiciones no razonables obstaculizarían el desarrollo de un mercado competitivo sostenible y no responderían al interés del usuario final.

La Comisión Nacional de los Mercados y la Competencia podrá imponer obligaciones a un operador para que facilite acceso a la obra civil, con independencia de si los bienes afectados por la obligación forman parte del mercado pertinente de acuerdo con el análisis del mercado, a condición de que la obligación sea necesaria y proporcionada;

e) acceso a elementos o a recursos específicos de las redes y recursos asociados y a su utilización, a efecto de satisfacer las solicitudes razonables de acceso a estos elementos y recursos, así como las relativas a su utilización, en aquellas situaciones en las que se considere que la denegación del acceso o unas condiciones no razonables de efecto análogo pueden constituir un obstáculo al desarrollo de un mercado competitivo sostenible a escala minorista y que no benefician a los usuarios finales;

f) control de precios, tales como la fijación de precios, la orientación de los precios en función de los costes y el establecimiento de una contabilidad de costes, con objeto de garantizar la formación de precios competitivos y evitar precios excesivos y márgenes no competitivos en detrimento de los usuarios finales.

La Comisión Nacional de los Mercados y la Competencia velará para que estos mecanismos de control de precios que se impongan sirvan para fomentar la competencia efectiva, los beneficios de los usuarios en términos de precios y calidad de los servicios y los intereses a largo plazo de los usuarios finales en relación con el despliegue y la adopción de redes de próxima generación, y en particular de redes de muy alta capacidad. Para favorecer la inversión por parte del operador, en particular en redes de próxima generación, la Comisión Nacional de los Mercados y la Competencia tendrá en cuenta la inversión efectuada, permitiendo una tasa razonable de rendimiento en relación con el capital correspondiente invertido, habida cuenta de todos los riesgos específicos de un nuevo proyecto de inversión concreto.

2. Cuando la Comisión Nacional de los Mercados y la Competencia estudie la conveniencia de imponer las obligaciones específicas de acceso previstas en la letra e) del apartado 1 de este artículo, podrá exigir al operador con peso significativo en el mercado que:

a) permita a terceros el acceso a elementos físicos específicos de la red y de los recursos asociados, según proceda, incluido el acceso desagregado al bucle y a los subbucles locales, y autorizar la utilización de los mismos;

b) conceda a terceros un acceso a elementos y servicios de redes específicos activos o virtuales;

c) negocie de buena fe con los operadores que soliciten el acceso;

d) no revoque una autorización de acceso a recursos previamente concedida;

e) preste servicios específicos en régimen de venta al por mayor para su reventa por terceros;

f) conceda libre acceso a interfaces técnicas, protocolos u otras tecnologías clave que sean indispensables para la interoperabilidad de los servicios o de servicios de redes virtuales;

g) facilite la coubicación u otras modalidades de uso compartido de recursos asociados;

h) preste servicios específicos necesarios para garantizar la interoperabilidad de servicios de extremo a extremo ofrecidos a los usuarios o la itinerancia en redes móviles;

i) proporcione acceso a sistemas de apoyo operativos o a sistemas informáticos similares necesarios para garantizar condiciones equitativas de competencia en la prestación de servicios;

j) interconecte redes o los recursos de estas;

k) proporcione acceso a servicios asociados tales como servicios de identidad, localización y presencia.

3. Cuando la Comisión Nacional de los Mercados y la Competencia estudie la conveniencia de imponer cualesquiera de las posibles obligaciones específicas previstas en el apartado 2, y en particular al evaluar, de conformidad con el principio de proporcionalidad, si dichas obligaciones deberían imponerse y de qué manera, analizará si otras formas de

acceso a los insumos al por mayor, bien en el mismo mercado o en un mercado mayorista relacionado, serían suficientes para resolver el problema identificado a nivel minorista en la búsqueda de los intereses de los usuarios finales. Dicho análisis incluirá ofertas de acceso comercial, un acceso regulado nuevo o un acceso regulado existente o previsto a otros insumos al por mayor. En particular, la Comisión Nacional de los Mercados y la Competencia habrá de considerar los siguientes elementos:

a) la viabilidad técnica y económica de utilizar o instalar recursos que compitan entre sí, a la vista del ritmo de desarrollo del mercado, teniendo en cuenta la naturaleza y el tipo de interconexión o acceso de que se trate, incluida la viabilidad de otros productos de acceso previo, como el acceso a conductos;

b) la evolución tecnológica previsible que afecte al diseño y a la gestión de la red;

c) la necesidad de garantizar una neutralidad tecnológica que permita a las partes diseñar y gestionar sus propias redes;

d) la viabilidad de proporcionar el acceso, en relación con la capacidad disponible;

e) la inversión inicial del propietario de los recursos, sin olvidar las inversiones públicas realizadas ni los riesgos inherentes a las inversiones, con especial atención a las inversiones en redes de muy alta capacidad y a los niveles de riesgo asociados a las mismas;

f) la necesidad de salvaguardar la competencia a largo plazo, prestando especial atención a la competencia económicamente eficiente basada en las infraestructuras y a unos modelos de negocio innovadores que apoyan la competencia sostenible, como los basados en inversiones conjuntas en redes;

g) cuando proceda, los derechos pertinentes en materia de propiedad intelectual;

h) el suministro de servicios paneuropeos.

Cuando la Comisión Nacional de los Mercados y la Competencia estudie, de conformidad con el artículo 17, la imposición de obligaciones previstas en las letras d) o e) del apartado 1 de este artículo, examinará si solo la imposición de obligaciones de acceso a las infraestructuras civiles sería un medio proporcionado para fomentar la competencia y los intereses del usuario final.

4. En circunstancias excepcionales y debidamente justificadas, la Comisión Nacional de los Mercados y la Competencia, previo sometimiento al mecanismo de notificación previsto en la disposición adicional novena, podrá imponer obligaciones específicas relativas al acceso o a la interconexión distintas a las enumeradas en el apartado 1.

A tal efecto, la Comisión Nacional de los Mercados y la Competencia presentará una solicitud a la Comisión Europea, que adoptará decisiones por las que se autorice o impida tomar tales medidas.

5. En la determinación e imposición, mantenimiento o modificación de las obligaciones específicas la Comisión Nacional de los Mercados y la Competencia optará por la forma menos intervencionista posible de resolver los problemas observados en el análisis del mercado, conforme al principio de proporcionalidad. En particular, tomará en cuenta los compromisos relativos a las condiciones de acceso o coinversión que hayan sido ofrecidos por los operadores que hayan sido declarados con peso significativo en el mercado y a los que se les haya otorgado carácter vinculante en los términos indicados en los artículos 19 y 20.

Las obligaciones específicas a imponer se basarán en la naturaleza del problema identificado, serán proporcionadas y estarán justificadas en el cumplimiento de los objetivos del artículo 3. Dichas obligaciones se mantendrán en vigor durante el tiempo estrictamente imprescindible.

6. La Comisión Nacional de los Mercados y la Competencia, en la imposición, mantenimiento, modificación o supresión de las obligaciones específicas tendrá en consideración el impacto de la nueva evolución del mercado que influya en la dinámica competitiva, para lo cual deberá tener en cuenta, entre otros, los acuerdos comerciales alcanzados entre operadores, incluidos los acuerdos de coinversión.

Si esa evolución no es suficientemente importante para necesitar un nuevo análisis del mercado, la Comisión Nacional de los Mercados y la Competencia valorará sin demora si es necesario revisar las obligaciones impuestas a los operadores que hayan sido declarados con peso significativo en el mercado y modificar cualquier decisión previa, incluidas la

supresión de obligaciones o la imposición de nuevas, previa realización de la notificación prevista en la disposición adicional novena.

7. Cuando la Comisión Nacional de los Mercados y la Competencia imponga obligaciones específicas a un operador de redes públicas de comunicaciones electrónicas para que facilite acceso podrá establecer determinadas condiciones técnicas u operativas al citado operador o a los beneficiarios de dicho acceso siempre que ello sea necesario para garantizar el funcionamiento normal de la red, conforme se establezca mediante real decreto. Las obligaciones de atenerse a normas o especificaciones técnicas concretas estarán de acuerdo con las normas a que se refiere el artículo 10.

8. Mediante real decreto, el Gobierno identificará las obligaciones específicas que la Comisión Nacional de los Mercados y la Competencia podrá imponer en los mercados de referencia considerados en este artículo y determinará las condiciones para su imposición, modificación o supresión.

Artículo 19. *Compromisos de acceso o coinversión ofrecidos por el operador.*

1. Los operadores que hayan sido calificados con peso significativo en el mercado podrán ofrecer a la Comisión Nacional de los Mercados y la Competencia compromisos relativos a las condiciones de acceso o de coinversión, o a ambas, que se aplicarán a sus redes en relación, entre otros asuntos, con:

a) los acuerdos de cooperación que sean pertinentes a efectos de la evaluación de la adecuación y proporcionalidad de las obligaciones específicas;

b) la coinversión en redes de muy alta capacidad en virtud del artículo siguiente, o

c) el acceso efectivo y no discriminatorio de terceros en virtud del artículo 26, tanto durante el período de ejecución de una separación voluntaria por parte de un operador integrado verticalmente como después de llevarse a cabo la separación propuesta.

La oferta de compromisos debe ser lo suficientemente detallada, en relación con el calendario y al alcance de la ejecución de los compromisos y a su duración, como para permitir su evaluación por parte de la Comisión Nacional de los Mercados y la Competencia. Tales compromisos podrán extenderse más allá de los plazos para la realización de los análisis del mercado previstos en el artículo 16.

2. A fin de evaluar los compromisos ofrecidos, la Comisión Nacional de los Mercados y la Competencia debe llevar a cabo, salvo cuando esos compromisos incumplan claramente uno de las condiciones o criterios pertinentes, una prueba de mercado, en particular, de las condiciones ofrecidas mediante la realización de una consulta pública a las partes interesadas, en particular los terceros directamente afectados. Los coinversores potenciales o los solicitantes de acceso podrán manifestar sus impresiones sobre si los compromisos propuestos cumplen o no las condiciones fijadas, y podrán proponer cambios a la oferta.

En la valoración de los compromisos, la Comisión Nacional de los Mercados y la Competencia, tendrá especialmente en cuenta:

a) las características que acrediten el carácter justo y razonable de los compromisos ofrecidos;

b) su apertura a todos los participantes del mercado;

c) la disponibilidad oportuna del acceso en condiciones justas, razonables y no discriminatorias, incluido el acceso a redes de muy alta capacidad, antes de que se pongan a la venta los servicios minoristas relacionados, y

d) la idoneidad general de los compromisos ofrecidos para permitir una competencia prolongada en los mercados descendentes y facilitar la cooperación en el despliegue y la adopción de redes de muy alta capacidad en interés de los usuarios finales.

Teniendo en cuenta todas las opiniones manifestadas en la consulta, la Comisión Nacional de los Mercados y la Competencia comunicará al operador que haya sido declarado con peso significativo en el mercado sus conclusiones preliminares sobre si los compromisos ofrecidos cumplen o no los objetivos, criterios y procedimientos previstos en el presente artículo y las condiciones en las que podría otorgar carácter vinculante a los citados compromisos. El operador podrá revisar su oferta inicial para tener en cuenta las

conclusiones preliminares de la Comisión Nacional de los Mercados y la Competencia y para cumplir los criterios establecidos.

3. La Comisión Nacional de los Mercados y la Competencia podrá adoptar una decisión por la que otorgue carácter vinculante a los compromisos, en su totalidad o en parte, por un período de tiempo específico, que podrá coincidir con la totalidad del período para el que se ofrecen, sin perjuicio de lo dispuesto en el artículo siguiente para la coinversión en redes de muy alta capacidad, teniendo en cuenta que en este último caso de coinversión dicho carácter vinculante tendrá una duración mínima de siete años.

El otorgamiento de carácter vinculante a los servicios se entenderá sin perjuicio de la aplicación del procedimiento de análisis del mercado previsto en el artículo 16 y la imposición de obligaciones con arreglo a los artículos 17 y 18. En particular, cuando la Comisión Nacional de los Mercados y la Competencia otorgue carácter vinculante a los compromisos, evaluará las consecuencias de tal decisión en el desarrollo del mercado y la idoneidad de las obligaciones que haya impuesto o, en ausencia de tales compromisos, hubiera pretendido imponer con arreglo a los anteriores artículos.

4. La Comisión Nacional de los Mercados y la Competencia controlará, supervisará y velará por la ejecución de los compromisos a los que haya otorgado carácter vinculante de la misma manera en que controle, supervise y vele por la ejecución de las obligaciones específicas y sopesará la prórroga una vez haya expirado el período de tiempo para el cual se les otorgó carácter vinculante.

En caso de que la Comisión Nacional de los Mercados y la Competencia concluya que el operador no ha cumplido los compromisos convertidos en vinculantes, podrá imponer las sanciones oportunas. La Comisión Nacional de los Mercados y la Competencia podrá asimismo reevaluar en estos casos las obligaciones impuestas al operador con peso significativo en el mercado, de conformidad con el artículo 18.

5. Las obligaciones relacionadas con los compromisos relativos a las condiciones de acceso y los acuerdos de coinversión se entenderán sin perjuicio de la aplicación a los mismos de la normativa en materia de competencia.

Artículo 20. *Compromisos de coinversión en redes de muy alta capacidad.*

1. Los operadores que hayan sido declarados con peso significativo en el mercado en uno o varios mercados pertinentes podrán ofrecer compromisos con arreglo al procedimiento previsto en el artículo anterior para abrir a la coinversión el despliegue de una nueva red de muy alta capacidad que consista en elementos de fibra óptica hasta los locales del usuario final o la estación base. Estos compromisos de coinversión pueden consistir, entre otros, en ofertas de propiedad conjunta, distribución de riesgos a largo plazo mediante cofinanciación o acuerdos de compra que generen derechos específicos de carácter estructural en favor de otros operadores de redes y servicios de comunicaciones electrónicas.

2. Cuando la Comisión Nacional de los Mercados y la Competencia evalúe esos compromisos, deberá determinar en particular si la oferta de coinversión cumple todas las condiciones siguientes:

a) se encuentra abierta a cualquier operador de redes o servicios de comunicaciones electrónicas en cualquier momento de la vida útil de la red;

b) permite a otros coinversores que sean operadores de redes y servicios de comunicaciones electrónicas competir de forma efectiva y prolongada en los mercados descendentes en los que ejerce su actividad el operador con peso significativo en el mercado, en condiciones que incluyan:

1.º condiciones justas, razonables y no discriminatorias que permitan acceder a la plena capacidad de la red en la medida en que sea objeto de coinversión;

2.º flexibilidad en términos del valor y del tiempo de la participación de cada coinversor;

3.º la posibilidad de aumentar dicha participación en el futuro, y

4.º derechos recíprocos conferidos por los coinversores tras el despliegue de la infraestructura objeto de coinversión;

c) el operador la hace pública al menos seis meses antes del inicio del despliegue de la nueva red, salvo que se trate de un operador exclusivamente mayorista en los términos indicados en el artículo 21;

d) los operadores solicitantes de acceso que no participen en la coinversión pueden beneficiarse desde el principio de la misma calidad y velocidad, de las mismas condiciones y de la misma penetración entre los usuarios finales disponible antes del despliegue, acompañados de un mecanismo de adaptación confirmado por la Comisión Nacional de los Mercados y la Competencia a las novedades que se produzcan en los mercados minoristas relacionados y que mantenga los incentivos para participar en la coinversión. El citado mecanismo velará por que los solicitantes de acceso puedan acceder a los elementos de muy alta capacidad de la red en un momento y sobre la base de condiciones transparentes y no discriminatorias que reflejen adecuadamente los niveles de riesgo asumidos por los correspondientes coinversores en las distintas etapas del despliegue y tengan en cuenta la situación de la competencia en los mercados minoristas;

e) satisface como mínimo los criterios que figuran en el anexo IV del Código Europeo de Comunicaciones electrónicas y se hace de buena fe.

3. Si la Comisión Nacional de los Mercados y la Competencia, teniendo en cuenta los resultados de la prueba de mercado llevada a cabo con arreglo al artículo 19, concluye que el compromiso de coinversión propuesto reúne las condiciones del apartado 2, otorgará carácter vinculante a los compromisos y no impondrá obligaciones específicas adicionales en lo que respecta a los elementos de la nueva red de muy alta capacidad que sean objeto de tales compromisos si al menos uno de los potenciales coinversores ha suscrito un acuerdo de coinversión con el operador con peso significativo en el mercado.

No obstante, la Comisión Nacional de los Mercados y la Competencia podrá, en circunstancias debidamente justificadas, imponer, mantener o adaptar obligaciones específicas en lo que respecta a las nuevas redes de muy alta capacidad con el fin de hacer frente a problemas de competencia importantes en mercados específicos cuando considere que, debido a las características específicas de tales mercados, no se podría hacer frente de otro modo a dichos problemas de competencia.

4. La Comisión Nacional de los Mercados y la Competencia deberá supervisar continuamente el cumplimiento de los compromisos de coinversión y podrá exigir al operador con peso significativo en el mercado que le facilite cada año declaraciones de cumplimiento.

5. Lo dispuesto en el presente artículo se entiende sin perjuicio de la facultad de la Comisión Nacional de los Mercados y la Competencia de resolver los conflictos que se le planteen entre empresas en el marco de un acuerdo de coinversión.

Artículo 21. *Operadores exclusivamente mayoristas.*

1. La Comisión Nacional de los Mercados y la Competencia, cuando designe a un operador que está ausente de los mercados minoristas de servicios de comunicaciones electrónicas como poseedora de peso significativo en uno o varios mercados al por mayor, examinará si dicho operador reúne las siguientes características:

a) todas las sociedades y unidades empresariales del operador, todas las sociedades controladas por el operador y cualquier accionista que ejerza un control sobre el operador, solamente tienen actividades, actuales y previstas para el futuro, en los mercados al por mayor de servicios de comunicaciones electrónicas y, por lo tanto, no tienen ninguna actividad en el mercado al por menor de servicios de comunicaciones electrónicas suministrados a los usuarios finales;

b) el operador no está obligado a negociar con un operador único e independiente que actúe en fases posteriores en un mercado al por menor de servicios de comunicaciones electrónicas prestados a usuarios finales, a causa de un acuerdo exclusivo o un acuerdo que de hecho equivalga a un acuerdo exclusivo.

2. A este tipo de operadores exclusivamente mayoristas, la Comisión Nacional de los Mercados y la Competencia solo les podrá imponer alguna de las obligaciones específicas de no discriminación o de acceso a elementos o a recursos específicos de las redes y recursos asociados y a su utilización, establecidas en el artículo 18.1.b) y e) o en relación con la fijación de precios justos y razonables si así lo justifica un análisis del mercado que incluya una evaluación prospectiva del comportamiento probable del operador con peso significativo en el mercado.

3. La Comisión Nacional de los Mercados y la Competencia revisará en cualquier momento las obligaciones impuestas al operador exclusivamente mayorista con arreglo al presente artículo si llega a la conclusión de que las condiciones establecidas en el apartado 1 han dejado de cumplirse y, en su caso, le impondrá las obligaciones específicas que corresponda. Los operadores exclusivamente mayoristas informarán sin demora indebida a la Comisión Nacional de los Mercados y la Competencia de cualquier cambio de circunstancias relacionado con el apartado 1, letras a) y b), del presente artículo.

4. La Comisión Nacional de los Mercados y la Competencia también revisará las obligaciones impuestas al operador conforme al presente artículo si, sobre la base de pruebas de las condiciones ofrecidas por el operador a sus clientes finales, llega a la conclusión de que han surgido o es probable que surjan problemas de competencia en detrimento de los usuarios finales y, en su caso, le impondrá las obligaciones específicas que corresponda.

Artículo 22. *Migración desde una infraestructura heredada.*

1. Los operadores que hayan sido declarados con peso significativo en uno o varios mercados pertinentes notificarán de antemano y de forma oportuna a la Comisión Nacional de los Mercados y la Competencia cuando tengan previsto clausurar o sustituir por una infraestructura nueva partes de la red, incluida la infraestructura existente necesaria para suministrar una red de cobre, que estén sujetas a las obligaciones contempladas en los capítulos IV y V de este título.

2. La Comisión Nacional de los Mercados y la Competencia velará por que el proceso de desmantelamiento y cierre o sustitución incluya un calendario y condiciones transparentes, incluido un plazo adecuado de notificación para la transición, y establezca la disponibilidad de productos alternativos de una calidad al menos comparable que faciliten el acceso a una infraestructura de red mejorada que sustituya a los elementos remplazados, si ello fuera necesario para preservar la competencia y los derechos de los usuarios finales.

3. La Comisión Nacional de los Mercados y la Competencia podrá retirar las obligaciones específicas impuestas en relación con los bienes cuya clausura o sustitución se propone, tras haberse asegurado de que el operador de acceso:

a) ha establecido las condiciones adecuadas para la migración, incluida la puesta a disposición de un producto de acceso alternativo de una calidad al menos comparable tal como era posible utilizando la infraestructura heredada que permita al solicitante de acceso llegar a los mismos usuarios finales, y

b) ha cumplido las condiciones y procedimientos que fueron notificados a la Comisión Nacional de los Mercados y la Competencia.

4. Este artículo se entenderá sin perjuicio de la disponibilidad de productos regulados impuesta por la Comisión Nacional de los Mercados y la Competencia en la infraestructura de red mejorada, de conformidad con los procedimientos establecidos en el marco de los procesos de análisis de mercados e imposición de obligaciones específicas.

Artículo 23. *Tarifas de terminación de llamadas de voz.*

1. En el caso de que la Comisión Europea no establezca a escala europea tarifas máximas de terminación de llamadas de voz en redes fijas o en redes móviles, o en ambas, la Comisión Nacional de los Mercados y la Competencia podrá realizar un análisis de mercado de los mercados de terminación de llamadas de voz para evaluar si es necesaria la imposición de obligaciones específicas, y, en su caso, podrá acordar su imposición. Si como resultado de tal análisis, la Comisión Nacional de los Mercados y la Competencia impone unas tarifas de terminación orientadas a los costes en un mercado respectivo, seguirá los principios, criterios y parámetros establecidos en el anexo III del Código Europeo de Comunicaciones Electrónicas.

2. La Comisión Nacional de los Mercados y la Competencia supervisará estrechamente y velará por el cumplimiento de la aplicación de las tarifas de terminación de llamadas de voz establecidas a escala europea. En cualquier momento, la Comisión Nacional de los Mercados y la Competencia podrá exigir a un operador de servicios de terminación de llamadas de voz que modifique la tarifa que cobra a otros operadores si no cumple las tarifas

máximas de terminación de llamadas de voz en redes fijas y en redes móviles establecidas por la Comisión Europea.

Artículo 24. *Obligaciones en mercados minoristas.*

1. La Comisión Nacional de los Mercados y la Competencia se abstendrá de aplicar mecanismos de control minorista a los mercados geográficos o minoristas en los que considere que existe una competencia efectiva.

2. No obstante lo anterior, la Comisión Nacional de los Mercados y la Competencia podrá imponer obligaciones apropiadas a los operadores que considere que tienen un peso significativo en un mercado minorista dado, cuando:

a) como resultado de un análisis de mercado, determine que un mercado minorista dado no es realmente competitivo, y

b) concluya que las obligaciones específicas impuestas en virtud de lo establecido en el artículo 18 no van a conllevar el logro de los objetivos establecidos en el artículo 3.

3. Las obligaciones impuestas con arreglo al apartado anterior podrán prohibir que los operadores considerados apliquen precios excesivos, obstaculicen la entrada de otros operadores en el mercado, falseen la competencia mediante el establecimiento de precios abusivos, favorezcan de manera excesiva a usuarios finales específicos o agrupen sus servicios de manera injustificada. Se podrán aplicar medidas apropiadas de limitación de los precios al público, de control de tarifas individuales o de orientación de las tarifas hacia costes o precios de mercados comparables, al objeto de proteger los intereses de los usuarios finales, fomentando al mismo tiempo una competencia real.

Las obligaciones impuestas se basarán en la naturaleza del problema detectado y serán proporcionadas y estarán justificadas habida cuenta de los objetivos establecidos en el artículo 3.

4. En los casos en que un operador vea sometidas a control sus tarifas al público u otros elementos pertinentes, la Comisión Nacional de los Mercados y la Competencia garantizará la aplicación de los sistemas necesarios y apropiados de contabilidad de costes. La Comisión Nacional de los Mercados y la Competencia podrá especificar el formato y la metodología contable que deberá emplearse, si bien un organismo independiente cualificado verificará la observancia del sistema de contabilidad de costes. La Comisión Nacional de los Mercados y la Competencia velará por que se publique anualmente una declaración de conformidad.

CAPÍTULO V

Separación funcional

Artículo 25. *Separación funcional obligatoria.*

1. Cuando la Comisión Nacional de los Mercados y la Competencia llegue a la conclusión de que las obligaciones específicas impuestas, en virtud de lo dispuesto en el artículo 18, no han bastado para conseguir una competencia efectiva y que sigue habiendo problemas de competencia importantes y persistentes o fallos del mercado en relación con mercados al por mayor de productos de acceso, podrá decidir la imposición, como medida excepcional, a los operadores con peso significativo en el mercado integrados verticalmente, de la obligación de traspasar las actividades relacionadas con el suministro al por mayor de productos de acceso a una unidad empresarial que actúe independientemente.

Esa unidad empresarial suministrará productos y servicios de acceso a todas las empresas, incluidas otras unidades empresariales de la sociedad matriz, en los mismos plazos, términos y condiciones, en particular en lo que se refiere a niveles de precios y de servicio, y mediante los mismos sistemas y procesos.

La imposición de la obligación de separación funcional prevista en el presente artículo se entenderá sin perjuicio de las medidas estructurales que se pudieran adoptar en aplicación de la normativa en materia de competencia.

2. Cuando la Comisión Nacional de los Mercados y la Competencia se proponga imponer una obligación de separación funcional, elaborará una propuesta que incluya:

a) motivos que justifiquen las conclusiones a las que ha llegado;

b) razones por las que hay pocas posibilidades, o ninguna, de competencia basada en la infraestructura en un plazo razonable;

c) un análisis del impacto previsto sobre la autoridad reguladora, sobre la empresa, particularmente en lo que se refiere a los trabajadores de la empresa separada y al sector de las comunicaciones electrónicas en su conjunto, sobre los incentivos para invertir en el sector en su conjunto, en especial por lo que respecta a la necesidad de garantizar la cohesión social y territorial, así como sobre otras partes interesadas, incluido en particular el impacto previsto sobre la competencia en infraestructuras y cualquier efecto negativo potencial sobre los consumidores, y

d) un análisis de las razones que justifiquen que esta obligación es el medio más adecuado para aplicar soluciones a los problemas de competencia o fallos del mercado que se hayan identificado.

3. El proyecto de medida incluirá los elementos siguientes:

a) la naturaleza y el grado precisos de la separación, especificando en particular el estatuto jurídico de la entidad empresarial separada;

b) una indicación de los activos de la entidad empresarial separada y de los productos o servicios que debe suministrar esta entidad;

c) los mecanismos de gobernanza para garantizar la independencia del personal empleado por la entidad empresarial separada y la estructura de incentivos correspondiente;

d) las normas para garantizar el cumplimiento de las obligaciones;

e) las normas para garantizar la transparencia de los procedimientos operativos, en particular de cara a otras partes interesadas, y

f) un programa de seguimiento para garantizar el cumplimiento, incluida la publicación de un informe anual.

4. La propuesta de imposición de la obligación de separación funcional, una vez que el Ministerio de Asuntos Económicos y Transformación Digital haya emitido informe sobre la misma, se presentará a la Comisión Europea.

5. Tras la decisión de la Comisión Europea, la Comisión Nacional de los Mercados y la Competencia llevará a cabo, de conformidad con el procedimiento previsto en el artículo 16, un análisis coordinado de los distintos mercados relacionados con la red de acceso. Sobre la base de su evaluación, previo informe de la Secretaría de Estado de Economía y Apoyo a la Empresa y de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, la Comisión Nacional de los Mercados y la Competencia impondrá, mantendrá, modificará o suprimirá las obligaciones específicas correspondientes.

Artículo 26. *Separación funcional voluntaria.*

1. En el supuesto de que un operador que haya sido declarado con peso significativo en uno o varios mercados pertinentes se proponga transferir sus activos de red de acceso local, o una parte sustancial de los mismos, a una persona jurídica separada de distinta propiedad, o establecer una entidad empresarial separada para suministrar a todos los operadores minoristas, incluidas sus propias divisiones minoristas, productos de acceso completamente equivalentes, deberá informar con al menos tres meses de antelación al Ministerio de Asuntos Económicos y Transformación Digital y a la Comisión Nacional de los Mercados y la Competencia.

El operador deberá informar también al Ministerio de Asuntos Económicos y Transformación Digital y a la Comisión Nacional de los Mercados y la Competencia de cualquier cambio de dicho propósito, así como del resultado final del proceso de separación.

2. Dicho operador también puede ofrecer compromisos respecto a las condiciones de acceso que aplicará a su red durante un período de ejecución y una vez se lleve a cabo la forma de separación propuesta, con el fin de garantizar el acceso efectivo y no discriminatorio de terceros. La oferta de compromisos incluirá detalles suficientes, incluso en términos de calendario de ejecución y duración, a fin de permitir a la Comisión Nacional de los Mercados y la Competencia que pueda llevar a cabo sus funciones. Tales compromisos podrán extenderse más allá del período máximo para las revisiones de los mercados relevantes establecidos en el artículo 16.

3. En el caso de que se realice la separación funcional voluntaria, la Comisión Nacional de los Mercados y la Competencia evaluará el efecto de la transacción prevista, junto con los compromisos propuestos en su caso, sobre las obligaciones reglamentarias impuestas a esa entidad, llevando a cabo, de conformidad con el procedimiento previsto en el artículo 16, un análisis coordinado de los distintos mercados relacionados con la red de acceso.

En dicho análisis, la Comisión Nacional de los Mercados y la Competencia tendrá en cuenta los compromisos ofrecidos por el operador, con especial atención a los objetivos establecidos en el artículo 3, para lo cual consultará a terceros y se dirigirá particularmente a aquellos terceros que estén directamente afectados por la transacción propuesta.

Sobre la base de su evaluación, previo informe de la Secretaría de Estado de Economía y Apoyo a la Empresa y de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, la Comisión Nacional de los Mercados y la Competencia impondrá, mantendrá, modificará o suprimirá las obligaciones específicas correspondientes, aplicando si procede las obligaciones del artículo 21. En su decisión, la Comisión Nacional de los Mercados y la Competencia podrá dar carácter vinculante a los compromisos ofrecidos por el operador, en su totalidad o en parte, pudiendo acordar que algunos o todos los compromisos sean vinculantes para la totalidad del período para el cual se ofrecen.

La Comisión Nacional de los Mercados y la Competencia supervisará la ejecución de los compromisos ofrecidos por el operador que haya considerado vinculantes y sopesará su prórroga, una vez expirado el período para el cual fueron inicialmente ofrecidos.

Artículo 27. *Obligaciones específicas adicionales a la separación funcional.*

Los operadores a los que se haya impuesto o que hayan decidido la separación funcional podrán estar sujetos a cualquiera de las obligaciones específicas enumeradas en el artículo 18 en cualquier mercado de referencia en que hayan sido declarados con peso significativo en el mercado.

CAPÍTULO VI

Resolución de conflictos

Artículo 28. *Resolución de conflictos en el mercado español.*

1. La Comisión Nacional de los Mercados y la Competencia resolverá los conflictos que se susciten, a petición de cualquiera de las partes interesadas, en relación con las obligaciones existentes en virtud de la presente ley y su normativa de desarrollo entre operadores, entre operadores y otras entidades que se beneficien de las obligaciones de acceso e interconexión o entre operadores y proveedores de recursos asociados.

2. La Comisión Nacional de los Mercados y la Competencia, previa audiencia de las partes, dictará resolución vinculante sobre los extremos objeto del conflicto, en el plazo de cuatro meses desde la recepción de toda la información, sin perjuicio de que puedan adoptarse medidas provisionales hasta el momento en que se dicte la resolución definitiva.

3. Al dictar la resolución que resuelva el conflicto, la Comisión Nacional de los Mercados y la Competencia perseguirá la consecución de los objetivos establecidos en el artículo 3. Las obligaciones que se puedan imponer en la resolución del conflicto deberán respetar los límites, requisitos y marco institucional establecidos en la presente ley y su normativa de desarrollo. La resolución del conflicto podrá impugnarse ante la jurisdicción contencioso-administrativa.

4. La posibilidad de presentar un conflicto ante la Comisión Nacional de los Mercados y la Competencia no impide que cualquiera de las partes pueda emprender acciones legales ante los órganos jurisdiccionales.

Artículo 29. *Resolución de conflictos transfronterizos.*

1. En caso de producirse un conflicto transfronterizo en el que una de las partes esté radicada en otro Estado miembro de la Unión Europea, salvo cuando el conflicto verse sobre la coordinación del espectro radioeléctrico, la Comisión Nacional de los Mercados y la Competencia, en caso de que cualquiera de las partes así lo solicite, coordinará sus

esfuerzos para encontrar una solución al conflicto con la otra u otras autoridades nacionales de reglamentación afectadas.

2. Cuando el conflicto afecte a las relaciones comerciales entre España y otro Estado miembro, la Comisión Nacional de los Mercados y la Competencia notificará el conflicto al ORECE con miras a alcanzar una resolución coherente del mismo, de conformidad con los objetivos establecidos en el artículo 3.

La Comisión Nacional de los Mercados y la Competencia y la otra u otras autoridades nacionales de reglamentación afectadas esperarán el dictamen del ORECE antes de tomar medida alguna para resolver el conflicto, sin perjuicio de que puedan adoptar, a petición de las partes o por iniciativa propia, medidas provisionales, con el fin de salvaguardar la competencia o de proteger los intereses de los usuarios finales.

La Comisión Nacional de los Mercados y la Competencia y la otra u otras autoridades nacionales de reglamentación afectadas deberán resolver el conflicto en el plazo de cuatro meses y, en todo caso, en el plazo de un mes a contar del dictamen del ORECE.

3. Las obligaciones que la Comisión Nacional de los Mercados y la Competencia y la otra u otras autoridades nacionales de reglamentación afectadas puedan imponer a una de las partes en la resolución del conflicto deberán ajustarse a la Directiva por la que se aprueba el Código Europeo de Comunicaciones Electrónicas, y tener en cuenta en la mayor medida posible el dictamen adoptado por el ORECE.

4. La posibilidad de presentar un conflicto transfronterizo ante la Comisión Nacional de los Mercados y la Competencia no impide que cualquiera de las partes pueda emprender acciones legales ante los órganos jurisdiccionales.

CAPÍTULO VII

Numeración

Artículo 30. *Principios generales.*

1. Para los servicios de comunicaciones electrónicas disponibles al público se proporcionarán los números que se necesiten para permitir su efectiva prestación, tomándose esta circunstancia en consideración en los planes nacionales correspondientes y en sus disposiciones de desarrollo.

2. Sin perjuicio de lo dispuesto en el apartado anterior, la regulación de los nombres de dominio de internet bajo el indicativo del país correspondiente a España («.es») se regirá por su normativa específica.

3. Corresponde al Gobierno la aprobación por real decreto de los planes nacionales de numeración, teniendo en cuenta las decisiones aplicables que se adopten en el seno de las organizaciones y los foros internacionales.

4. Corresponde al Ministerio de Asuntos Económicos y Transformación Digital, previo informe de la Comisión Nacional de los Mercados y la Competencia, la elaboración de las propuestas de planes nacionales para su elevación al Gobierno, y el desarrollo normativo de estos planes que podrán establecer condiciones asociadas a la utilización de los recursos públicos de numeración, en particular la designación del servicio para el que se utilizarán estos recursos, incluyendo cualquier requisito relacionado con el suministro de dicho servicio.

5. Corresponde a la Comisión Nacional de los Mercados y la Competencia el otorgamiento de los derechos de uso de los recursos públicos regulados en los planes nacionales de numeración.

No se limitará el número de derechos de uso de los recursos de numeración que deban otorgarse salvo cuando resulte necesario para garantizar un uso eficiente de los recursos de numeración.

Los procedimientos para el otorgamiento de estos derechos serán abiertos, objetivos, no discriminatorios, proporcionados y transparentes. Estos procedimientos se establecerán mediante real decreto.

Las decisiones relativas a los otorgamientos de derechos de uso se adoptarán, comunicarán y harán públicas en el plazo máximo de tres semanas desde la recepción de la solicitud completa, salvo cuando se apliquen procedimientos de selección comparativa o

competitiva, en cuyo caso, el plazo máximo será de seis semanas desde el fin del plazo de recepción de ofertas. En estas decisiones se especificará si el titular de los derechos puede cederlos, y en qué condiciones.

Transcurrido el plazo máximo sin haberse notificado la resolución expresa, se podrá entender desestimada la solicitud por silencio administrativo. Asimismo, también se harán públicas las decisiones que se adopten relativas a la cancelación de derechos de uso.

6. Los operadores que presten servicios de comunicaciones vocales u otros servicios que permitan efectuar y recibir llamadas a números del plan nacional de numeración deberán cursar las llamadas que se efectúen a los rangos de numeración telefónica nacional y, cuando permitan llamadas internacionales, a todos los números proporcionados en la Unión Europea, incluidos los de los planes nacionales de numeración de otros Estados miembros, y a otros rangos de numeración internacional, en los términos que se especifiquen en los planes nacionales de numeración o en sus disposiciones de desarrollo, sin perjuicio del derecho del usuario de desconexión de determinados servicios.

7. El otorgamiento de derechos de uso de los recursos públicos de numeración regulados en los planes nacionales no supondrá el otorgamiento de más derechos que los de su utilización conforme a lo que se establece en esta ley.

8. Los operadores a los que se haya concedido el derecho de uso de recursos de numeración no podrán discriminar a otros operadores en lo que se refiere a los recursos de numeración utilizados para dar acceso a sus servicios.

9. Todos los operadores y, en su caso, los fabricantes y los comerciantes estarán obligados a tomar las medidas necesarias para el cumplimiento de las decisiones que se adopten por el Ministerio de Asuntos Económicos y Transformación Digital en materia de numeración.

10. Empresas distintas de los operadores de redes públicas o de servicios de comunicaciones electrónicas disponibles al público tendrán, en los términos que determine la normativa de desarrollo de la ley, acceso a los recursos públicos regulados en los planes nacionales para la prestación de servicios específicos. Esta normativa podrá prever, cuando esté justificado, el otorgamiento de derechos de uso de números a estas empresas para determinados rangos que a tal efecto se definan en los planes nacionales o en sus disposiciones de desarrollo. Dichas empresas deberán demostrar su capacidad para gestionar los recursos de numeración y cumplir con cualquier requisito pertinente que se establezca. La Comisión Nacional de los Mercados y la Competencia podrá acordar no mantener la concesión de los derechos de uso de recursos de numeración a dichas empresas si se demuestra que existe un riesgo de agotamiento de los recursos de numeración.

11. El número «00» es el código común de acceso a la red telefónica internacional.

Será posible adoptar o mantener mecanismos específicos para el uso de servicios de comunicaciones interpersonales basados en numeración entre lugares adyacentes situados a ambos lados de las fronteras entre España y resto de Estados miembros.

Asimismo, se podrá acordar con otros Estados miembros compartir un plan de numeración común para todas las categorías de números o para algunas categorías específicas.

12. El Gobierno apoyará la armonización de determinados números o series de números concretos dentro de la Unión Europea cuando ello promueva al mismo tiempo el funcionamiento del mercado interior y el desarrollo de servicios paneuropeos.

Artículo 31. *Planes nacionales de numeración.*

1. Los planes nacionales de numeración y sus disposiciones de desarrollo designarán los servicios para los que puedan utilizarse los números, incluido cualquier requisito relacionado con la prestación de tales servicios y las condiciones asociadas a su uso, que serán proporcionadas y no discriminatorias. Asimismo, los planes nacionales y sus disposiciones de desarrollo podrán incluir los principios de fijación de precios y los precios máximos que puedan aplicarse a los efectos de garantizar la protección de los consumidores.

2. El contenido de los citados planes y el de los actos derivados de su desarrollo y gestión serán públicos, salvo en lo relativo a materias que puedan afectar a la seguridad nacional.

3. A fin de cumplir con las obligaciones y recomendaciones internacionales o para garantizar la disponibilidad suficiente de números, la persona titular del Ministerio de Asuntos Económicos y Transformación Digital podrá, mediante orden que se publicará con la debida antelación a su entrada en vigor, y previo informe de la Comisión Nacional de los Mercados y la Competencia, modificar la estructura y la organización de los planes nacionales o, en ausencia de éstos o de planes específicos para cada servicio, establecer medidas sobre la utilización de los recursos numéricos y alfanuméricos necesarios para la prestación de los servicios. Se habrán de tener en cuenta, a tales efectos, los intereses de los afectados y los gastos de adaptación que, de todo ello, se deriven para los operadores y para los usuarios.

4. Los planes nacionales de numeración o sus disposiciones de desarrollo podrán establecer procedimientos de selección competitiva o comparativa para el otorgamiento de derechos de uso de números y nombres con valor económico excepcional o que sean particularmente apropiados para la prestación de determinados servicios de interés general. Estos procedimientos respetarán los principios de publicidad, concurrencia y no discriminación para todas las partes interesadas.

5. Los planes nacionales de numeración destinada a la prestación de los servicios de tarificación adicional se aprobarán por Orden del Ministerio de Asuntos Económicos y Transformación Digital. En dichos planes se incluirán las condiciones directamente asociadas al uso de la numeración para dichos servicios, entre ellas:

a) La atribución de los servicios concretos a que se dedicará cada rango de numeración.

b) Los precios máximos minoristas para los servicios, así como para cada uno de los rangos y subrangos de numeración atribuidos o habilitados a estos servicios y su posible distribución por intervalos.

c) La obligatoriedad de incorporar una locución inicial o mensaje previo informativo, que el usuario deberá recibir antes del inicio o contratación del servicio.

d) Los distintos modos de marcación de la numeración admisibles para la contratación del servicio.

e) La duración máxima de la llamada telefónica para la prestación de estos servicios.

6. No podrán ser objeto de regulación en los planes a los que se refiere el apartado anterior aquellos aspectos no directamente relacionados con el uso de la numeración, por ser relativos a la protección de los derechos de los consumidores y usuarios y, en consecuencia, regidos por la legislación general de esta materia. Entre ellos se pueden citar:

a) La publicidad de los servicios de tarificación adicional, en cualquiera de sus formas.

b) El contenido de los servicios, así como la especial protección de determinados grupos de población, como la infancia y la juventud.

c) Las reglas de los concursos u otro tipo de juegos o sorteos de azar que puedan desarrollarse a través de llamadas o mensajes de tarificación adicional.

Artículo 32. *Acceso a números o servicios.*

1. En la medida que resulte necesario para la consecución de los objetivos establecidos en el artículo 3 y, en particular, para salvaguardar los derechos e intereses de los usuarios, mediante real decreto o en los Planes Nacionales de numeración y sus disposiciones de desarrollo, podrán establecerse requisitos sobre capacidades o funcionalidades mínimas que deberán cumplir determinados tipos de servicios.

2. Los operadores que suministren redes públicas de comunicaciones o presten servicios vocales disponibles al público, siempre que sea técnica y económicamente posible, adoptarán las medidas que sean necesarias para que los usuarios finales puedan tener acceso a los servicios utilizando números no geográficos en la Unión Europea, y que puedan tener acceso, con independencia de la tecnología y los dispositivos utilizados por el operador, a todos los números proporcionados en la Unión Europea, incluidos los de los planes nacionales de numeración de otros Estados miembros, y los Números Universales Internacionales de Llamada Gratuita.

3. Asimismo, mediante real decreto, previo informe de la Comisión Nacional de los Mercados y la Competencia, se establecerán las condiciones en las que los operadores de redes públicas de comunicaciones electrónicas o servicios de comunicaciones electrónicas disponibles al público lleven a cabo el bloqueo de acceso a números o servicios, siempre

que esté justificado por motivos de tráfico no permitido y de tráfico irregular con fines fraudulentos, y los casos en que los prestadores de servicios de comunicaciones electrónicas retengan los correspondientes ingresos por interconexión u otros servicios. La Comisión Nacional de los Mercados y la Competencia podrá ordenar el bloqueo de acceso a números o servicios por motivos de tráfico irregular con fines fraudulentos cuando tengan su origen en un conflicto entre operadores en materia de acceso o interconexión que le sea planteado por dichos operadores. En ningún caso podrá exigirse al amparo de este apartado el bloqueo a servicios no incluidos en el ámbito de aplicación de esta ley, como los servicios de la Sociedad de la Información regulados en la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

4. La persona titular del Ministerio de Asuntos Económicos y Transformación Digital podrá establecer que, por razones de protección de los derechos de los usuarios finales de servicios de comunicaciones electrónicas, en especial, relacionadas con la facturación y las tarifas que se aplican en la prestación de determinados servicios, algunos números o rangos de numeración sólo sean accesibles previa petición expresa del usuario, en las condiciones que se fijen mediante orden.

Artículo 33. *Conservación de los números por los usuarios finales y fomento de la provisión inalámbrica para facilitar el cambio de operador.*

1. Los operadores garantizarán, de conformidad con lo establecido en el artículo 65.1.e) y en el artículo 70, que los usuarios finales con números del plan nacional de numeración puedan conservar, previa solicitud, los números que les hayan sido asignados, con independencia del operador que preste el servicio. Mediante real decreto se fijarán los supuestos a los que sea de aplicación la conservación de números, así como los aspectos técnicos y administrativos necesarios para que esta se lleve a cabo. En aplicación de este real decreto y su normativa de desarrollo, la Comisión Nacional de los Mercados y la Competencia podrá fijar, mediante circular, características y condiciones para la conservación de los números.

2. Los costes derivados de la actualización de los elementos de la red y de los sistemas necesarios para hacer posible la conservación de los números deberán ser sufragados por cada operador sin que, por ello, tengan derecho a percibir indemnización alguna. Los demás costes que produzca la conservación de los números telefónicos se repartirán, a través del oportuno acuerdo, entre los operadores afectados por el cambio. A falta de acuerdo, resolverá la Comisión Nacional de los Mercados y la Competencia. Los precios de interconexión para la aplicación de las facilidades de conservación de los números habrán de estar orientados en función de los costes. No se podrán imponer cuotas directas a los usuarios finales por la conservación del número.

3. Cuando sea técnicamente viable, se fomentará la provisión inalámbrica para facilitar el cambio de operadores de redes o servicios de comunicaciones electrónicas por parte de los usuarios finales, en particular los operadores y usuarios finales de servicios de máquina a máquina.

Artículo 34. *Números armonizados para los servicios armonizados europeos de valor social.*

1. El Ministerio de Asuntos Económicos y Transformación Digital promoverá el conocimiento por la población de los números armonizados europeos que comienzan por las cifras 116, garantizará que los usuarios finales tengan acceso gratuito a las llamadas a esa numeración y fomentará la prestación en España de los servicios de valor social para los que están reservados tales números, poniéndolos a disposición de los interesados en su prestación.

2. El Ministerio de Asuntos Económicos y Transformación Digital adoptará las iniciativas pertinentes para que los usuarios finales con discapacidad puedan tener el mejor acceso posible a los servicios prestados a través de los números armonizados europeos que comienzan por las cifras 116. En la atribución de tales números, dicho Ministerio establecerá las condiciones que faciliten el acceso a los servicios que se presten a través de ellos por los usuarios finales con discapacidad.

Entre las referidas condiciones podrán incluirse, en función del servicio en concreto de valor social que se trate, la de posibilitar la comunicación total a través de voz, texto y video para que las personas con discapacidad sensorial no se queden excluidas.

3. Las Administraciones públicas competentes en la regulación o supervisión de cada uno de los servicios que se presten a través de los números armonizados europeos que comienzan por las cifras 116 velarán por que los ciudadanos reciban una información adecuada sobre la existencia y utilización de estos servicios de valor social.

TÍTULO III

Obligaciones de servicio público y derechos y obligaciones de carácter público en el suministro de redes y en la prestación de servicios de comunicaciones electrónicas

CAPÍTULO I

Obligaciones de servicio público

Sección 1.ª Delimitación

Artículo 35. *Delimitación de las obligaciones de servicio público.*

1. Este capítulo tiene por objeto garantizar la existencia de servicios de comunicaciones electrónicas disponibles al público de adecuada calidad en todo el territorio nacional a través de una competencia y una libertad de elección reales, y hacer frente a las circunstancias en que las necesidades de los usuarios finales no se vean atendidas de manera satisfactoria por el mercado.

2. Los operadores se sujetarán al régimen de obligaciones de servicio público y de carácter público, de acuerdo con lo establecido en este título.

3. La imposición de obligaciones de servicio público perseguirá la consecución de los objetivos establecidos en el artículo 3 y podrá recaer sobre los operadores que obtengan derechos de ocupación del dominio público o de la propiedad privada, de derechos de uso del dominio público radioeléctrico, de derechos de uso de recursos públicos de numeración o que ostenten la condición de operador con peso significativo en un determinado mercado de referencia. Cuando se impongan obligaciones de servicio público, se aplicará con carácter supletorio el régimen establecido para la concesión de servicios en la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.

4. El cumplimiento de las obligaciones de servicio público en la instalación y explotación de redes públicas y en la prestación de servicios de comunicaciones electrónicas para los que aquéllas sean exigibles se efectuará con respeto a los principios de igualdad, transparencia, no discriminación, continuidad, adaptabilidad, disponibilidad, accesibilidad universal y permanencia y conforme a los términos y condiciones que mediante real decreto se determinen.

5. Corresponde al Ministerio de Asuntos Económicos y Transformación Digital el control y el ejercicio de las facultades de la Administración relativas a las obligaciones de servicio público y de carácter público a que se refiere este artículo.

6. Cuando el Ministerio de Asuntos Económicos y Transformación Digital constate que cualquiera de los servicios a que se refiere este artículo se está prestando en competencia, en condiciones de precio, cobertura y calidad de servicio similares a aquellas en que los operadores designados deben prestarlas, podrá, previo informe de la Comisión Nacional de los Mercados y la Competencia y audiencia a los interesados, determinar el cese de su prestación como obligación de servicio público y, en consecuencia, de la financiación prevista para tales obligaciones.

Artículo 36. *Categorías de obligaciones de servicio público.*

Los operadores están sometidos a las siguientes categorías de obligaciones de servicio público:

a) el servicio universal en los términos contenidos en la sección 2.ª de este capítulo;
b) otras obligaciones de servicio público impuestas por razones de interés general, en la forma y con las condiciones establecidas en la sección 3.ª de este capítulo.

Sección 2.ª El servicio universal

Artículo 37. *Concepto y ámbito de aplicación.*

1. Se entiende por servicio universal el conjunto definido de servicios cuya prestación se garantiza para todos los consumidores con independencia de su localización geográfica, en condiciones de neutralidad tecnológica, con una calidad determinada y a un precio asequible.
Los servicios incluidos en el servicio universal, en los términos y condiciones que mediante real decreto se determinen por el Gobierno, son:

a) Servicio de acceso adecuado y disponible a una internet de banda ancha a través de una conexión subyacente en una ubicación fija, que deberá soportar el conjunto mínimo de servicios a que se refiere el anexo III. La velocidad mínima de acceso a una internet de banda ancha se fija en 10 Mbit por segundo en sentido descendente.
Mediante real decreto, teniendo en cuenta la evolución social, económica y tecnológica y las condiciones de competencia en el mercado, se modificará la velocidad mínima de acceso a una internet de banda ancha, en particular, escalando dicha velocidad mínima a 30 Mbit por segundo en sentido descendente tan pronto como sea posible en función de la extensión de las redes y del estado de la técnica, así como se determinarán sus características y parámetros técnicos, y se podrá modificar el conjunto mínimo de servicios que deberá soportar el servicio de acceso a una internet de banda ancha a que se refiere el anexo III.
b) Servicios de comunicaciones vocales a través de una conexión subyacente en una ubicación fija.

2. La conexión subyacente en una ubicación fija podrá limitarse al soporte de los servicios de las comunicaciones vocales, cuando así lo solicite el consumidor.
3. Mediante real decreto, se podrá ampliar el ámbito de aplicación del servicio universal o de algunos de sus elementos u obligaciones a los usuarios finales que sean microempresas y pequeñas y medianas empresas y organizaciones sin ánimo de lucro.
4. Las condiciones en que se preste el servicio universal deberán perseguir reducir al mínimo las distorsiones del mercado, en particular cuando la prestación de servicios se realice a precios o en condiciones divergentes de las prácticas comerciales normales, salvaguardando al mismo tiempo el interés público.
5. El Gobierno, de conformidad con la normativa comunitaria, podrá revisar la determinación de los servicios que forman parte del servicio universal, así como el alcance de las obligaciones de servicio universal.

Artículo 38. *Asequibilidad del servicio universal.*

1. Los precios minoristas en los que se prestan los servicios incluidos dentro del servicio universal han de ser asequibles y no deben impedir a los consumidores con rentas bajas o con necesidades sociales especiales acceder a tales servicios. A tales efectos, mediante real decreto, previo informe de la Comisión Nacional de los Mercados y la Competencia, se determinarán las características sociales y de poder adquisitivo correspondientes para determinar de que los consumidores tienen rentas bajas o necesidades sociales especiales.
2. La Comisión Nacional de los Mercados y la Competencia, en coordinación con el Ministerio de Asuntos Económicos y Transformación Digital y con el departamento ministerial competente en materia de protección de los consumidores y usuarios, supervisará la evolución y el nivel de la tarificación al público de los servicios incluidos en el servicio universal, bien sean prestados por todos los operadores o bien sean prestados por el

operador u operadores designados, en particular en relación con los niveles nacionales de precios al consumo y de rentas.

3. Todos los operadores que presten servicios de acceso a una internet de banda ancha y los servicios de comunicaciones vocales que se presten a través de una conexión subyacente en una ubicación fija deben ofrecer a los consumidores con rentas bajas o con necesidades sociales especiales opciones o paquetes de tarifas que difieran de las aplicadas en condiciones normales de explotación comercial en condiciones transparentes, públicas y no discriminatorias. A tal fin se podrá exigir a dichos operadores que apliquen limitaciones de precios, tarifas comunes, equiparación geográfica u otros regímenes similares. Mediante real decreto se podrá establecer si los operadores, en el marco de estas opciones o paquetes de tarifas, disponen de la posibilidad o no de fijar un volumen máximo de datos a transmitir en el servicio de acceso a internet de banda ancha.

Entre estas opciones o paquetes de tarifas deberán figurar un abono social para servicios de comunicaciones vocales que se presten a través de una conexión subyacente en una ubicación fija, un abono social para servicios de acceso a una internet de banda ancha que se presten a través de una conexión subyacente en una ubicación fija y un abono social que incluya de manera empaquetada ambos servicios.

La Comisión Nacional de los Mercados y la Competencia, previo informe de la Secretaría de Estado de Economía y Apoyo a la Empresa y de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, podrá exigir la modificación o supresión de las opciones o paquetes de tarifas ofrecidas por los operadores a los consumidores con rentas bajas o con necesidades sociales especiales, para lo cual podrá exigir a dichos operadores que apliquen limitaciones de precios, tarifas comunes, equiparación geográfica u otros regímenes similares. En todo caso, el Ministerio de Asuntos Económicos y Transformación Digital podrá proponer a la Comisión Nacional de los Mercados y la Competencia la modificación o supresión de las opciones o paquetes de tarifas ofrecidas por los operadores a los consumidores con rentas bajas o con necesidades sociales especiales.

4. Cuando el cumplimiento de las obligaciones de asequibilidad por todos los operadores impuestas en el apartado anterior dé lugar a una carga administrativa o financiera excesiva, la Comisión Nacional de los Mercados y la Competencia, previo informe de la Secretaría de Estado de Economía y Apoyo a la Empresa y de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, podrá decidir, con carácter excepcional, imponer la obligación de ofrecer estas opciones o paquetes de tarifas solo al operador u operadores designados en virtud de lo establecido en el artículo 40, en cuyo caso deberá velar por que todos los consumidores de renta baja o con necesidades sociales especiales disfruten de una variedad de operadores que ofrecen opciones de tarifas adecuadas a sus necesidades, a menos que ello resulte imposible o cree una carga organizativa o financiera adicional excesiva.

5. Los consumidores con rentas bajas o con necesidades sociales especiales que puedan beneficiarse de dichas opciones o paquetes de tarifas tienen el derecho de celebrar un contrato y que su número siga disponible durante un período adecuado y se evite la desconexión injustificada del servicio.

6. Los operadores que tengan la obligación de ofrecer opciones o paquetes de tarifas a consumidores con rentas bajas o con necesidades sociales especiales deberán publicarlas adecuadamente, garantizar que sean transparentes, que las apliquen de conformidad con el principio de no discriminación y mantener informados a la Comisión Nacional de los Mercados y la Competencia y al Ministerio de Asuntos Económicos y Transformación Digital.

7. Mediante real decreto, se podrán establecer requisitos para que el servicio de acceso a una internet de banda ancha y los servicios de comunicaciones vocales que se presten a través de una conexión subyacente en una ubicación no fija resulten asequibles en aras de garantizar la plena participación social y económica de los consumidores en la sociedad.

8. Todos los operadores que presten servicios de acceso a una internet de banda ancha y los servicios de comunicaciones vocales que se presten a través de una conexión subyacente en una ubicación fija en el marco del servicio universal deben garantizar el cumplimiento de las condiciones de velocidad de acceso a internet y de prestación de los servicios normativamente establecidas así como las que figuren en los correspondientes contratos con los consumidores.

Artículo 39. *Accesibilidad del servicio universal.*

1. Los consumidores con discapacidad deben tener un acceso a los servicios incluidos en el servicio universal a un nivel equivalente al que disfrutan otros consumidores.

2. A tal efecto, se podrán imponer como obligación de servicio universal medidas específicas con vistas a garantizar que los equipos terminales conexos y los equipos y servicios específicos que favorecen un acceso equivalente, incluidos, en su caso, los servicios de conversión a texto y los servicios de conversación total en modo texto, estén disponibles y sean asequibles.

3. Mediante real decreto se adoptarán medidas a fin de garantizar que los consumidores con discapacidad también puedan beneficiarse de la capacidad de elección de operadores de que disfruta la mayoría de los consumidores.

Artículo 40. *Designación de los operadores encargados de la prestación del servicio universal.*

1. Cuando la prestación de cualquiera de los servicios integrantes del servicio universal en una ubicación fija no quede garantizada por las circunstancias normales de explotación comercial, el Ministerio de Asuntos Económicos y Transformación Digital designará uno o más operadores para que satisfagan todas las solicitudes razonables de acceso a los servicios integrantes del servicio universal y garanticen su prestación eficiente en las partes afectadas del territorio nacional a efecto de asegurar su disponibilidad en todo el territorio nacional. A estos efectos podrán designarse operadores diferentes para la prestación de los distintos servicios del servicio universal y abarcar distintas zonas o partes del territorio nacional.

2. El sistema de designación de operadores encargados de garantizar la prestación de los servicios integrantes del servicio universal se establecerá mediante real decreto, con sujeción a los principios de eficiencia, objetividad, transparencia y no discriminación sin excluir a priori la designación de ningún operador. En todo caso, contemplará un mecanismo de licitación pública para la prestación de dichos servicios. Estos procedimientos de designación garantizarán que la prestación de los servicios incluidos en el servicio universal se haga de manera rentable y se podrán utilizar como medio para determinar el coste neto derivado de las obligaciones asignadas, a los efectos de lo dispuesto en el artículo 42.2.

3. Cuando uno de los operadores designados para la prestación del servicio universal se proponga entregar una parte sustancial o la totalidad de sus activos de red de acceso local a una persona jurídica separada de distinta propiedad, informará con la debida antelación al Ministerio de Asuntos Económicos y Transformación Digital a fin de evaluar las repercusiones de la operación prevista en el suministro en una ubicación fija de los servicios incluidos en el servicio universal. El Ministerio de Asuntos Económicos y Transformación Digital, como consecuencia de la evaluación realizada, podrá imponer, modificar o suprimir obligaciones a dicho operador designado.

4. El Ministerio de Asuntos Económicos y Transformación Digital podrá establecer objetivos de rendimiento aplicables al operador u operadores designados para la prestación del servicio universal.

5. El Ministerio de Asuntos Económicos y Transformación Digital notificará a la Comisión Europea las obligaciones de servicio universal impuestas al operador u operadores designados para el cumplimiento de obligaciones de servicio universal, así como los cambios relacionados con dichas obligaciones o con el operador u operadores designados.

Artículo 41. *Control del gasto.*

1. Los operadores que cumplan obligaciones de servicio universal en virtud de lo establecido en los artículos 37 a 40, deberán ofrecer a los consumidores las facilidades y los servicios específicos determinados mediante real decreto, que incluirán, en todo caso, los relacionados en la parte A del anexo VI del Código Europeo de Comunicaciones Electrónicas, a fin de permitir a los consumidores el seguimiento y control de sus propios gastos.

2. Dichos operadores deberán implantar un sistema para evitar la desconexión injustificada del servicio de comunicaciones vocales o de un servicio de acceso adecuado a

internet de banda ancha de los consumidores con rentas bajas o con necesidades sociales especiales, incluido un mecanismo adecuado para verificar el interés por seguir utilizando el servicio.

3. Los consumidores que se beneficien del cumplimiento de las obligaciones de servicio universal no pueden verse obligados al pago de facilidades o servicios adicionales que no sean necesarios o que resulten superfluos para el servicio solicitado.

Artículo 42. *Coste y financiación del servicio universal.*

1. Todas las obligaciones que se incluyen en el servicio universal estarán sujetas a los mecanismos de financiación que se establecen en este artículo.

2. La Comisión Nacional de los Mercados y la Competencia determinará si la obligación de la prestación del servicio universal puede implicar una carga injusta para los operadores obligados a su prestación.

En caso de que se considere que puede existir dicha carga injusta, el coste neto de prestación del servicio universal será determinado periódicamente por la Comisión Nacional de los Mercados y la Competencia de acuerdo con los procedimientos de designación previstos en el artículo 40.2 o en función del ahorro neto que el operador conseguiría si no tuviera la obligación de prestar el servicio universal.

Para la determinación de este ahorro neto la Comisión Nacional de los Mercados y la Competencia desarrollará y publicará una metodología de acuerdo con los criterios que se establezcan mediante real decreto.

Las cuentas y demás información en que se base el cálculo del ahorro neto serán objeto de auditoría por parte de la Comisión Nacional de los Mercados y la Competencia. Los resultados y las conclusiones de la auditoría se pondrán a disposición del público.

3. El coste neto de la obligación de prestación del servicio universal será financiado por un mecanismo de reparto, en condiciones de transparencia, distorsión mínima del mercado, no discriminación y proporcionalidad, por aquellos operadores que obtengan por el suministro de redes públicas o la prestación de servicios de comunicaciones electrónicas disponibles al público unos ingresos brutos de explotación anuales superiores a 100 millones de euros. Esta cifra podrá ser actualizada o modificada mediante real decreto acordado en Consejo de Ministros, previo informe de la Comisión Nacional de los Mercados y la Competencia, en función de la evolución del mercado y de las cuotas que los distintos operadores tienen en cada momento en el mercado.

4. Una vez fijado este coste, la Comisión Nacional de los Mercados y la Competencia determinará las aportaciones que correspondan a cada uno de los operadores con obligaciones de contribución a la financiación del servicio universal.

Dichas aportaciones, así como, en su caso, las deducciones y exenciones aplicables, se verificarán de acuerdo con las condiciones que se establezcan por real decreto.

Las aportaciones recibidas se depositarán en el Fondo nacional del servicio universal.

5. El Fondo nacional del servicio universal tiene por finalidad garantizar la financiación del servicio universal.

El Fondo nacional del servicio universal ha de utilizar un sistema transparente y neutro de recaudación de contribuciones que evite el peligro de la doble imposición de contribuciones sobre operaciones soportadas y repercutidas por los operadores.

Los activos en metálico procedentes de los operadores con obligaciones de contribuir a la financiación del servicio universal se depositarán en este fondo, en una cuenta específica designada a tal efecto. Los gastos de gestión de esta cuenta serán deducidos de su saldo, y los rendimientos que este genere, si los hubiere, minorarán la contribución de los aportantes.

En la cuenta podrán depositarse aquellas aportaciones que sean realizadas por cualquier persona física o jurídica que desee contribuir, desinteresadamente, a la financiación de cualquier prestación propia del servicio universal.

Los operadores sujetos a obligaciones de prestación del servicio universal recibirán de este fondo la cantidad correspondiente al coste neto que les supone dicha obligación, calculado según el procedimiento establecido en este artículo.

La Comisión Nacional de los Mercados y la Competencia se encargará de la gestión del Fondo nacional del servicio universal. Mediante real decreto se determinará su estructura,

organización, mecanismos de control y la forma y plazos en los que se realizarán las aportaciones.

6. Mediante real decreto podrá preverse la existencia de un mecanismo de compensación directa entre operadores para aquellos casos en que la magnitud del coste no justifique los costes de gestión del fondo nacional del servicio universal.

Sección 3.ª Otras obligaciones de servicio público

Artículo 43. *Otras obligaciones de servicio público.*

1. El Gobierno podrá, por necesidades de la seguridad nacional, de la defensa nacional, de la seguridad pública, seguridad vial o de los servicios que afecten a la seguridad de las personas o a la protección civil, imponer otras obligaciones de servicio público distintas de las de servicio universal a los operadores.

2. El Gobierno podrá, asimismo, imponer otras obligaciones de servicio público, previo informe de la Comisión Nacional de los Mercados y la Competencia, así como de la administración territorial competente, motivadas por:

a) razones de cohesión territorial;

b) razones de extensión del uso de nuevos servicios y tecnologías, en especial a la sanidad, a la educación, a la acción social y a la cultura;

c) por la necesidad de facilitar la comunicación entre determinados colectivos que se encuentren en circunstancias especiales y estén insuficientemente atendidos con la finalidad de garantizar la suficiencia de su oferta.

3. Mediante real decreto se regulará el procedimiento de imposición de las obligaciones a las que se refiere el apartado anterior y su forma de financiación.

CAPÍTULO II

Derechos de los operadores y despliegue de redes públicas de comunicaciones electrónicas

Sección 1.ª Derechos de los operadores a la ocupación del dominio público, a ser beneficiarios en el procedimiento de expropiación forzosa y al establecimiento a su favor de servidumbres y de limitaciones a la propiedad

Artículo 44. *Derecho de ocupación de la propiedad privada.*

1. Los operadores tendrán derecho, en los términos de este capítulo, a la ocupación de la propiedad privada cuando resulte estrictamente necesario para la instalación, despliegue y explotación de la red en la medida prevista en el proyecto técnico presentado y siempre que no existan otras alternativas técnica o económicamente viables, ya sea a través de su expropiación forzosa o mediante la declaración de servidumbre forzosa de paso para la instalación, despliegue y explotación de infraestructura de redes públicas de comunicaciones electrónicas. En ambos casos tendrán la condición de beneficiarios en los expedientes que se tramiten, conforme a lo dispuesto en la legislación sobre expropiación forzosa.

Los operadores asumirán los costes a los que hubiera lugar por esta ocupación.

La ocupación de la propiedad privada se llevará a cabo tras la instrucción y resolución por el Ministerio de Asuntos Económicos y Transformación Digital del oportuno procedimiento, en que deberán cumplirse todos los trámites y respetarse todas las garantías establecidas a favor de los titulares afectados en la legislación de expropiación forzosa.

2. La aprobación por el órgano competente del Ministerio de Asuntos Económicos y Transformación Digital del proyecto técnico para la ocupación de propiedad privada llevará implícita, en cada caso concreto, la declaración de utilidad pública y la necesidad de ocupación para la instalación de redes públicas de comunicaciones electrónicas, a efectos de lo previsto en la legislación de expropiación forzosa.

3. Con carácter previo a la aprobación del proyecto técnico, se recabará informe del órgano de la Comunidad Autónoma competente en materia de ordenación del territorio, que habrá de ser emitido en el plazo máximo de treinta días hábiles desde su solicitud. Si el

proyecto afecta a un área geográfica relevante o pudiera tener afecciones ambientales, este plazo será ampliado hasta tres meses. Asimismo, se recabará informe de los Ayuntamientos afectados sobre compatibilidad del proyecto técnico con la ordenación urbanística vigente, que deberá ser emitido en el plazo de treinta días hábiles desde la recepción de la solicitud.

4. En las expropiaciones que se lleven a cabo para la instalación de redes públicas de comunicaciones electrónicas ligadas de manera específica al cumplimiento de obligaciones de servicio público se seguirá el procedimiento especial de urgencia establecido en la Ley de Expropiación Forzosa, cuando así se haga constar en la resolución del órgano competente del Ministerio de Asuntos Económicos y Transformación Digital que apruebe el oportuno proyecto técnico.

Artículo 45. *Derecho de ocupación del dominio público.*

Los operadores tendrán derecho, en los términos de este capítulo, a la ocupación del dominio público necesario para el establecimiento de la red pública de comunicaciones electrónicas de que se trate.

Los titulares del dominio público garantizarán el acceso de todos los operadores a dicho dominio en condiciones neutrales, objetivas, transparentes, equitativas y no discriminatorias, sin que en ningún caso pueda establecerse derecho preferente o exclusivo alguno de acceso u ocupación de dicho dominio público en beneficio de un operador determinado o de una red concreta de comunicaciones electrónicas. En particular, la ocupación o el derecho de uso de dominio público para la instalación o explotación de una red no podrá ser otorgado o asignado mediante procedimientos de licitación.

Se podrán celebrar acuerdos o convenios entre los operadores y los titulares o gestores del dominio público para facilitar el despliegue simultáneo de otros servicios, que deberán ser gratuitos para las Administraciones y los ciudadanos, vinculados a la mejora del medio ambiente, de la salud pública, de la seguridad pública y de la protección civil ante catástrofes naturales o para mejorar o facilitar la vertebración y cohesión territorial y urbana o contribuir a la sostenibilidad de la logística urbana.

La propuesta de acuerdo o convenio para la ocupación del dominio público deberá incluir un plan de despliegue e instalación con el contenido previsto en el artículo 49.9 de esta ley. Transcurrido el plazo máximo de tres meses desde su presentación, el acuerdo o convenio se entenderá aprobado si no hubiera pronunciamiento expreso en contra justificado adecuadamente.

Artículo 46. *Ubicación compartida y uso compartido de la propiedad pública o privada.*

1. Los operadores de redes públicas de comunicaciones electrónicas podrán celebrar de manera voluntaria acuerdos entre sí para determinar las condiciones para la ubicación o el uso compartido de sus elementos de red y recursos asociados, así como la utilización compartida del dominio público o la propiedad privada, con plena sujeción a la normativa de defensa de la competencia.

Las Administraciones públicas fomentarán la celebración de acuerdos voluntarios entre operadores para la ubicación compartida y el uso compartido de elementos de red y recursos asociados, así como la utilización compartida del dominio público o la propiedad privada, en particular con vistas al despliegue de elementos de las redes de comunicaciones electrónicas de alta y muy alta capacidad.

2. La ubicación compartida de elementos de red y recursos asociados y la utilización compartida del dominio público o la propiedad privada también podrá ser impuesta de manera obligatoria a los operadores que hayan ejercido el derecho a la ocupación de la propiedad pública o privada. A tal efecto, en los términos en que mediante real decreto se determine, el Ministerio de Asuntos Económicos y Transformación Digital, previo trámite de audiencia a los operadores afectados y de manera motivada, podrá imponer, con carácter general o para casos concretos, la utilización compartida del dominio público o la propiedad privada en que se van a establecer las redes públicas de comunicaciones electrónicas o el uso compartido de los elementos de red y recursos asociados, determinando, en su caso, los criterios para compartir los gastos que produzca la ubicación o el uso compartido.

Cuando una Administración Pública competente considere que por razones de medio ambiente, salud pública, seguridad pública u ordenación urbana y territorial se justifica la

imposición de la utilización compartida del dominio público o la propiedad privada, podrá instar de manera motivada al Ministerio de Asuntos Económicos y Transformación Digital el inicio del procedimiento establecido en el párrafo anterior. En estos casos, antes de que el Ministerio de Asuntos Económicos y Transformación Digital imponga la utilización compartida del dominio público o la propiedad privada, el citado departamento ministerial deberá realizar un trámite para que la Administración Pública competente que ha instado el procedimiento pueda efectuar alegaciones por un plazo de quince días hábiles.

3. Las medidas adoptadas de conformidad con el presente artículo deberán ser objetivas, transparentes, no discriminatorias y proporcionadas. Cuando proceda, estas medidas se aplicarán de forma coordinada con las Administraciones competentes correspondientes y con la Comisión Nacional de los Mercados y la Competencia.

Artículo 47. *Otras servidumbres y limitaciones a la propiedad.*

1. La protección del dominio público radioeléctrico tiene como finalidades su aprovechamiento óptimo, evitar su degradación y el mantenimiento de un adecuado nivel de calidad en el funcionamiento de los distintos servicios de radiocomunicaciones y aquellos otros que hacen uso del dominio público radioeléctrico.

El Ministerio de Asuntos Económicos y Transformación Digital podrá establecer las limitaciones a la propiedad y a la intensidad de campo eléctrico y las servidumbres que resulten necesarias para la protección radioeléctrica de determinadas instalaciones o para asegurar el adecuado funcionamiento de estaciones o instalaciones radioeléctricas utilizadas para la prestación de servicios públicos, por motivos de seguridad pública o cuando así sea necesario en virtud de acuerdos internacionales, en los términos de la disposición adicional segunda y las normas de desarrollo de esta ley.

2. Asimismo, el Ministerio de Asuntos Económicos y Transformación Digital podrá imponer límites a los derechos de uso del dominio público radioeléctrico para la protección de otros servicios o bienes jurídicamente protegidos prevalentes o de servicios públicos que puedan verse afectados por la utilización de dicho dominio público, en los términos que mediante real decreto se determinen. En la imposición de estos límites se debe efectuar un previo trámite de audiencia a los titulares de los derechos de uso del dominio público radioeléctrico que pueden verse afectados y se deberán respetar los principios de transparencia y publicidad.

Artículo 48. *Estudios geográficos.*

1. El Ministerio de Asuntos Económicos y Transformación Digital efectuará anualmente un estudio sobre el alcance y extensión de las redes de banda ancha, incluidas las redes de muy alta capacidad, con un nivel de desagregación local o incluso inferior.

El estudio geográfico incluirá información suficiente sobre la calidad del servicio y los parámetros de este último.

La información que no esté sujeta a confidencialidad comercial será accesible de conformidad con la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público. El Ministerio de Asuntos Económicos y Transformación Digital informará a las empresas que proporcionen información en base a este artículo sobre el hecho de que la misma ha sido compartida con otras autoridades públicas, en su caso.

2. El Ministerio de Asuntos Económicos y Transformación Digital incluirá en el estudio geográfico una previsión sobre el alcance y extensión que van a tener las redes de banda ancha, incluidas las redes de muy alta capacidad, para un período determinado, con el grado de desagregación que estime oportuno.

Esta previsión será sometida a una consulta pública en la página web del Ministerio de Asuntos Económicos y Transformación Digital. En ella, a partir de una base de datos geográfica proporcionada por el Ministerio de Asuntos Económicos y Transformación Digital, los operadores declararán cualquier intención de desplegar redes de banda ancha que ofrezca velocidades de descarga o transferencia de al menos 100 Mbps o redes de muy alta capacidad o de mejorar o extender significativamente sus redes hasta alcanzar una velocidad de descarga o transferencia de al menos 100 Mbps. Esta declaración de intenciones supone un compromiso en firme por parte del operador, de forma que su incumplimiento por causas imputables al operador que produzca un perjuicio al interés

público en el diseño de planes nacionales de banda ancha, en la determinación de obligaciones de cobertura ligadas a los derechos de uso del espectro radioeléctrico o en la verificación de la disponibilidad de servicios en el marco de la obligación de servicio universal, o bien un perjuicio a otro operador, podrá ser sancionada en los términos previstos en el título VIII.

A la vista de las aportaciones efectuadas en la consulta pública, de las declaraciones de intenciones efectuadas y de otra información de que pueda disponer, el Ministerio de Asuntos Económicos y Transformación Digital elaborará y publicará una previsión definitiva sobre el alcance y extensión que van a tener las redes de banda ancha, incluidas las redes de muy alta capacidad, para un período determinado. Esta previsión incluirá toda la información pertinente, en particular, información del despliegue planeado de redes de muy alta capacidad y mejoras o extensiones de redes con una velocidad de descarga o transferencia de al menos 100 Mbps.

3. A efectos de la elaboración de estos estudios geográficos, el Ministerio de Asuntos Económicos y Transformación Digital podrá solicitar la información necesaria y ajustada a este fin, en los términos indicados en el artículo 9, a las personas físicas o jurídicas que suministren redes o presten servicios de comunicaciones electrónicas, así como a aquellos otros agentes que intervengan en este mercado o en mercados y sectores estrechamente relacionados, con el grado de desagregación oportuno.

El Ministerio de Asuntos Económicos y Transformación Digital también solicitará información para la elaboración de estos estudios geográficos al resto de Administraciones públicas, en particular, a las Comunidades Autónomas, Diputaciones provinciales y Ayuntamientos.

4. La información contenida en los estudios geográficos servirá de base para la elaboración de los planes nacionales de banda ancha o de conectividad digital, que priorizarán la cobertura de los núcleos de población más pequeños y del entorno rural, para el diseño de ayudas públicas para el despliegue de redes públicas de comunicaciones electrónicas, para la aplicación de la normativa sobre ayudas estatales, para la determinación de obligaciones de cobertura ligadas a los derechos de uso del espectro radioeléctrico y la verificación de la disponibilidad de servicios en el marco de la obligación de servicio universal.

La Comisión Nacional de los Mercados y la Competencia y otras Administraciones públicas también podrán basarse en la información que proporcionen los estudios geográficos para el ejercicio de sus funciones. A tal efecto, podrán solicitar al Ministerio de Asuntos Económicos y Transformación Digital la información oportuna, priorizando el acceso y tratamiento de dicha información por medios electrónicos. El Ministerio de Asuntos Económicos y Transformación Digital y la Comisión Nacional de los Mercados y la Competencia colaborarán en la determinación y desglose de la información a obtener para confeccionar los estudios geográficos, a efectos de que puedan ejercer con mayor eficacia y eficiencia sus funciones.

Sección 2.ª Normativa de las Administraciones públicas que afecte a la instalación o explotación de redes públicas de comunicaciones electrónicas

Artículo 49. *Colaboración entre Administraciones públicas en la instalación o explotación de las redes públicas de comunicaciones electrónicas.*

1. La Administración General del Estado y las demás Administraciones públicas deberán colaborar a través de los mecanismos previstos en la presente ley y en el resto del ordenamiento jurídico, a fin de hacer efectivo el derecho de los operadores de comunicaciones electrónicas de ocupar la propiedad pública y privada para realizar el despliegue de redes públicas de comunicaciones electrónicas.

2. Las redes públicas de comunicaciones electrónicas y recursos asociados coadyuvan a la consecución de un fin de interés general, constituyen equipamiento de carácter básico y su previsión en los instrumentos de planificación urbanística tiene el carácter de determinaciones estructurantes. Su instalación y despliegue constituyen obras de interés general.

3. La normativa elaborada por las Administraciones públicas que afecte a la instalación o explotación de las redes públicas de comunicaciones electrónicas y los instrumentos de planificación territorial o urbanística deberán, en todo caso, contemplar la necesidad de instalar y explotar redes públicas de comunicaciones electrónicas y recursos asociados y reconocer el derecho de ocupación del dominio público o la propiedad privada para la instalación, despliegue o explotación de dichas redes y recursos asociados de conformidad con lo dispuesto en este título.

4. La normativa elaborada por las Administraciones públicas que afecte a la instalación o explotación de las redes públicas de comunicaciones electrónicas y recursos asociados y los instrumentos de planificación territorial o urbanística deberán recoger las disposiciones necesarias para permitir, impulsar o facilitar la instalación o explotación de infraestructuras de redes de comunicaciones electrónicas y recursos asociados en su ámbito territorial, en particular, para garantizar la libre competencia en la instalación o explotación de redes y recursos asociados y en la prestación de servicios de comunicaciones electrónicas y la disponibilidad de una oferta suficiente de lugares y espacios físicos en los que los operadores decidan ubicar sus infraestructuras.

De esta manera, dicha normativa o instrumentos de planificación territorial o urbanística no podrán establecer restricciones absolutas o desproporcionadas al derecho de ocupación del dominio público y privado de los operadores ni imponer soluciones tecnológicas concretas, itinerarios o ubicaciones concretas en los que instalar infraestructuras de red de comunicaciones electrónicas. En este sentido, cuando una condición pudiera implicar la imposibilidad de llevar a cabo la ocupación del dominio público o la propiedad privada, el establecimiento de dicha condición deberá estar plenamente justificado por razones de medio ambiente, seguridad pública u ordenación urbana y territorial e ir acompañado de las alternativas necesarias para garantizar el derecho de ocupación de los operadores y su ejercicio en igualdad de condiciones.

Las Administraciones públicas contribuirán a garantizar y hacer real una oferta suficiente de lugares y espacios físicos en los que los operadores decidan ubicar sus infraestructuras identificando dichos lugares y espacios físicos en los que poder cumplir el doble objetivo de que los operadores puedan ubicar sus infraestructuras de redes de comunicaciones electrónicas, así como la obtención de un despliegue de las redes ordenado desde el punto de vista territorial.

5. La normativa elaborada por las Administraciones públicas en el ejercicio de sus competencias que afecte a la instalación o explotación de las redes públicas de comunicaciones electrónicas y recursos asociados y los instrumentos de planificación territorial o urbanística deberán cumplir con lo dispuesto en la normativa sectorial de telecomunicaciones. En particular, deberán respetar los parámetros y requerimientos técnicos esenciales necesarios para garantizar el funcionamiento de las distintas redes y servicios de comunicaciones electrónicas, establecidos en la disposición adicional decimotercera y en las normas reglamentarias aprobadas en materia de telecomunicaciones, y los límites en los niveles de emisión radioeléctrica tolerable fijados por el Estado.

En el ejercicio de su iniciativa normativa, cuando esta afecte a la instalación o explotación de redes públicas de comunicaciones electrónicas, las Administraciones públicas actuarán de acuerdo con los principios de necesidad, proporcionalidad, seguridad jurídica, transparencia, accesibilidad, simplicidad y eficacia.

6. La normativa elaborada por las Administraciones públicas en el ejercicio de sus competencias que afecte a la instalación y explotación de las redes públicas de comunicaciones electrónicas y recursos asociados y los instrumentos de planificación territorial o urbanística deberán cumplir, al menos, los siguientes requisitos:

a) ser publicadas en un diario oficial del ámbito correspondiente a la Administración competente, así como en la página web de dicha Administración Pública y, en todo caso, ser accesibles por medios electrónicos;

b) prever un procedimiento rápido, sencillo, eficiente y no discriminatorio de resolución de las solicitudes de ocupación, que no podrá exceder de cuatro meses contados a partir de la presentación de la solicitud, salvo en caso de expropiación. No obstante lo anterior, la obtención de permisos, autorizaciones o licencias relativos a las obras civiles necesarias para desplegar elementos de las redes públicas de comunicaciones electrónicas de alta o

muy alta capacidad, las Administraciones públicas concederán o denegarán los mismos dentro de los tres meses siguientes a la fecha de recepción de la solicitud completa. Excepcionalmente, y mediante resolución motivada comunicada al solicitante tras expirar el plazo inicial, este plazo podrá extenderse un mes más, no pudiendo superar el total de cuatro meses desde la fecha de recepción de la solicitud completa. La Administración Pública competente podrá fijar unos plazos de resolución inferiores;

c) garantizar la transparencia de los procedimientos y que las normas aplicables fomenten una competencia leal y efectiva entre los operadores;

d) garantizar el respeto de los límites impuestos a la intervención administrativa en esta ley en protección de los derechos de los operadores. En particular, la exigencia de documentación que los operadores deban aportar deberá ser motivada, tener una justificación objetiva, ser proporcionada al fin perseguido y limitarse a lo estrictamente necesario y al principio de reducción de cargas administrativas.

7. Los operadores no tendrán obligación de aportar la documentación o información de cualquier naturaleza que ya obre en poder de la Administración. El Ministerio de Asuntos Económicos y Transformación Digital establecerá, mediante real decreto, la forma en que se facilitará a las Administraciones públicas la información que precisen para el ejercicio de sus propias competencias.

8. Los operadores deberán hacer uso de las canalizaciones subterráneas o en el interior de las edificaciones que permitan la instalación y explotación de redes públicas de comunicaciones electrónicas.

En los casos en los que no existan dichas canalizaciones o no sea posible o razonable su uso por razones técnicas los operadores podrán efectuar despliegues aéreos siguiendo los previamente existentes.

Igualmente, en los mismos casos, los operadores podrán efectuar por fachadas despliegue de cables y equipos que constituyan redes públicas de comunicaciones electrónicas y sus recursos asociados, si bien para ello deberán utilizar, en la medida de lo posible, los despliegues, canalizaciones, instalaciones y equipos previamente instalados, debiendo adoptar las medidas oportunas para minimizar el impacto visual.

Los despliegues aéreos y por fachadas no podrán realizarse en casos justificados de edificaciones del patrimonio histórico-artístico con la categoría de bien de interés cultural declarada por las administraciones competentes o que puedan afectar a la seguridad pública.

9. Para la instalación o explotación de las estaciones o infraestructuras radioeléctricas y recursos asociados en dominio privado no podrá exigirse por parte de las Administraciones públicas competentes la obtención de licencia o autorización previa de obras, instalaciones, de funcionamiento o de actividad, de carácter medioambiental ni otras de clase similar o análogas, excepto en edificaciones del patrimonio histórico-artístico con la categoría de bien de interés cultural declarada por las autoridades competentes o cuando ocupen una superficie superior a 300 metros cuadrados, computándose a tal efecto toda la superficie incluida dentro del vallado de la estación o instalación o, tratándose de instalaciones de nueva construcción, tengan impacto en espacios naturales protegidos.

Para la instalación o explotación de redes públicas de comunicaciones electrónicas fijas o de estaciones o infraestructuras radioeléctricas y sus recursos asociados en dominio privado distintas de las señaladas en el párrafo anterior, no podrá exigirse por parte de las Administraciones públicas competentes la obtención de licencia o autorización previa de obras, instalaciones, de funcionamiento o de actividad, o de carácter medioambiental, ni otras licencias o aprobaciones de clase similar o análogas que sujeten a previa autorización dicha instalación, en el caso de que el operador haya presentado voluntariamente a la Administración Pública competente para el otorgamiento de la licencia o autorización un plan de despliegue o instalación de red de comunicaciones electrónicas, en el que se contemplen dichas infraestructuras o estaciones, y siempre que el citado plan haya sido aprobado por dicha administración.

Para la instalación y despliegue de redes públicas de comunicaciones electrónicas y sus recursos asociados que deban realizarse en dominio público, las Administraciones públicas podrán establecer, cada una en el ámbito exclusivo de sus competencias y para todos o

algunos de los casos, que la tramitación se realice mediante declaración responsable o comunicación previa.

Los planes de despliegue o instalación son documentos de carácter descriptivo e informativo, no debiendo tener un grado de detalle propio de un proyecto técnico y su presentación es potestativa para los operadores. Su contenido se considera confidencial.

En el plan de despliegue o instalación, el operador efectuará una mera previsión de los supuestos en los que se pueden efectuar despliegues aéreos o por fachadas de cables y equipos en los términos indicados en el apartado anterior.

Este plan de despliegue o instalación a presentar por el operador se sujetará al contenido y deberá respetar las condiciones técnicas exigidas mediante real decreto acordado en Consejo de Ministros.

El plan de despliegue o instalación de red pública de comunicaciones electrónicas se entenderá aprobado si, transcurrido el plazo máximo de tres meses desde su presentación, la Administración Pública competente no ha dictado resolución expresa. La Administración Pública competente podrá fijar un plazo de resolución inferior.

Tanto para la aprobación de un plan de despliegue o instalación como para el otorgamiento, en su caso, de una autorización o licencia, la Administración competente sólo podrá exigir al operador documentación asociada a su ámbito competencial, que sea razonable y proporcional al fin perseguido y que no se encuentre ya en poder de la propia administración.

Las licencias o autorizaciones previas que, de acuerdo con los párrafos anteriores, no puedan ser exigidas, serán sustituidas por declaraciones responsables, de conformidad con lo establecido en el artículo 69 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, relativas al cumplimiento de las previsiones legales establecidas en la normativa vigente. En todo caso, el declarante deberá estar en posesión del justificante de pago del tributo correspondiente cuando sea preceptivo.

La declaración responsable deberá contener una manifestación explícita del cumplimiento de aquellos requisitos que resulten exigibles de acuerdo con la normativa vigente, incluido, en su caso, estar en posesión de la documentación que así lo acredite.

Cuando deban realizarse diversas actuaciones relacionadas con la infraestructura o estación radioeléctrica, las declaraciones responsables se tramitarán conjuntamente siempre que ello resulte posible.

La presentación de la declaración responsable, con el consiguiente efecto de habilitación a partir de ese momento para ejecutar la instalación, no prejuzgará en modo alguno la situación y efectivo acomodo de las condiciones de la infraestructura o estación radioeléctrica a la normativa aplicable, ni limitará el ejercicio de las potestades administrativas de comprobación, inspección, sanción, y, en general, de control que a la Administración en cualquier orden, estatal, autonómico o local, le estén atribuidas por el ordenamiento sectorial aplicable en cada caso.

La inexactitud, falsedad u omisión, de carácter esencial, en cualquier dato, manifestación o documento que se acompañe o incorpore a una declaración responsable, o la no presentación de la declaración responsable determinará la imposibilidad de explotar la instalación y, en su caso, la obligación de retirarla desde el momento en que se tenga constancia de tales hechos, sin perjuicio de las responsabilidades penales, civiles o administrativas a que hubiera lugar.

Reglamentariamente se establecerán los elementos de la declaración responsable que tendrán dicho carácter esencial.

10. Para la instalación o explotación de los puntos de acceso inalámbrico para pequeñas áreas y sus recursos asociados, en los términos definidos por la normativa europea, no se requerirá ningún tipo de concesión, autorización o licencia nueva o modificación de la existente o declaración responsable o comunicación previa a las Administraciones públicas competentes por razones de ordenación del territorio o urbanismo, salvo en los supuestos de edificios o lugares de valor arquitectónico, histórico o natural que estén protegidos de acuerdo con la legislación nacional o, en su caso, por motivos de seguridad pública o seguridad nacional.

La instalación de los puntos de acceso inalámbrico para pequeñas áreas y sus recursos asociados no está sujeta a la exigencia de tributos por ninguna Administración Pública, excepto la tasa general de operadores y sin perjuicio de lo dispuesto en el artículo 52.

11. En el caso de que sobre una infraestructura de red pública de comunicaciones electrónicas, fija o móvil, incluidas las estaciones radioeléctricas de comunicaciones electrónicas y sus recursos asociados, ya esté ubicada en dominio público o privado, se realicen actuaciones de innovación tecnológica o adaptación técnica que supongan la incorporación de nuevo equipamiento o la realización de emisiones radioeléctricas en nuevas bandas de frecuencias o con otras tecnologías, sin cambiar la ubicación de los elementos de soporte ni variar los elementos de obra civil y mástil, no se requerirá ningún tipo de concesión, autorización o licencia nueva o modificación de la existente o declaración responsable o comunicación previa a las Administraciones públicas competentes por razones de ordenación del territorio, urbanismo, dominio público hidráulico, de carreteras o medioambientales, siempre y cuando no suponga un riesgo estructural para la infraestructura sobre la que se asienta la red.

12. Cuando las Administraciones públicas elaboren proyectos que impliquen la variación en la ubicación de una infraestructura o un elemento de la red de transmisión de comunicaciones electrónicas, deberán dar audiencia previa al operador titular de la infraestructura afectada, a fin de que realice las alegaciones pertinentes sobre los aspectos técnicos, económicos y de cualquier otra índole respecto a la variación proyectada.

13. Si las Administraciones públicas reguladoras o titulares del dominio público ostentan la propiedad, total o parcial, o ejercen el control directo o indirecto de operadores que explotan redes públicas de comunicaciones electrónicas o servicios de comunicaciones electrónicas disponibles para el público, deberán mantener una separación estructural entre dichos operadores y los órganos encargados de la regulación y gestión de los derechos de utilización del dominio público correspondiente.

Artículo 50. *Mecanismos de colaboración entre el Ministerio de Asuntos Económicos y Transformación Digital y las Administraciones públicas para la instalación y explotación de las redes públicas de comunicaciones electrónicas.*

1. El Ministerio de Asuntos Económicos y Transformación Digital y las Administraciones públicas tienen los deberes de recíproca información y de colaboración y cooperación mutuas en el ejercicio de sus actuaciones de regulación y que puedan afectar a las telecomunicaciones, según lo establecido por el ordenamiento vigente.

Esta colaboración se articulará, entre otros, a través de los mecanismos establecidos en los siguientes apartados, que podrán ser complementados mediante acuerdos de coordinación y cooperación entre el Ministerio de Asuntos Económicos y Transformación Digital y las Administraciones públicas competentes, garantizando en todo caso un trámite de audiencia para los interesados.

2. Los órganos encargados de los procedimientos de aprobación, modificación o revisión de los instrumentos de planificación territorial o urbanística que afecten a la instalación o explotación de las redes públicas de comunicaciones electrónicas y recursos asociados deberán recabar el oportuno informe del Ministerio de Asuntos Económicos y Transformación Digital. Dicho informe versará sobre la adecuación de dichos instrumentos de planificación con la presente ley y con la normativa sectorial de telecomunicaciones y sobre las necesidades de redes públicas de comunicaciones electrónicas en el ámbito territorial a que se refieran.

El referido informe preceptivo será previo a la aprobación del instrumento de planificación de que se trate y tendrá carácter vinculante en lo que se refiere a su adecuación a la normativa sectorial de telecomunicaciones, en particular, al régimen jurídico de las telecomunicaciones establecido por la presente ley y su normativa de desarrollo, y a las necesidades de redes públicas de comunicaciones electrónicas, debiendo señalar expresamente los puntos y aspectos respecto de los cuales se emite con ese carácter vinculante.

El Ministerio de Asuntos Económicos y Transformación Digital emitirá el informe en un plazo máximo de tres meses. Sin perjuicio de lo dispuesto en el artículo 80.4 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones

Públicas, transcurrido dicho plazo, el informe se entenderá emitido con carácter favorable y podrá continuarse con la tramitación del instrumento de planificación.

A falta de solicitud del preceptivo informe, no podrá aprobarse el correspondiente instrumento de planificación territorial o urbanística en lo que se refiere al ejercicio de las competencias estatales en materia de telecomunicaciones.

En el caso de que el informe no sea favorable, los órganos encargados de la tramitación de los procedimientos de aprobación, modificación o revisión de los instrumentos de planificación territorial o urbanística dispondrán de un plazo máximo de un mes, a contar desde la recepción del informe, para remitir al Ministerio de Asuntos Económicos y Transformación Digital sus alegaciones al informe, motivadas por razones de medio ambiente, salud pública, seguridad pública u ordenación urbana y territorial.

El Ministerio de Asuntos Económicos y Transformación Digital, a la vista de las alegaciones presentadas, emitirá un nuevo informe en el plazo máximo de un mes a contar desde la recepción de las alegaciones. Sin perjuicio de lo dispuesto en el artículo 80.4 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, transcurrido dicho plazo, el informe se entenderá emitido con carácter favorable y podrá continuarse con la tramitación del instrumento de planificación. El informe tiene carácter vinculante, de forma que si el informe vuelve a ser no favorable, no podrá aprobarse el correspondiente instrumento de planificación territorial o urbanística en lo que se refiere al ejercicio de las competencias estatales en materia de telecomunicaciones.

3. Mediante orden de la persona titular del Ministerio de Asuntos Económicos y Transformación Digital se podrá establecer la forma en que han de solicitarse los informes a que se refiere el apartado anterior y la información a facilitar por parte del órgano solicitante, en función del tipo de instrumento de planificación territorial o urbanística, pudiendo exigirse a las Administraciones públicas competentes su tramitación por vía electrónica.

4. En la medida en que la instalación y despliegue de las redes de comunicaciones electrónicas y recursos asociados constituyen obras de interés general, el conjunto de Administraciones públicas tiene la obligación de facilitar el despliegue de infraestructuras de redes de comunicaciones electrónicas en su ámbito territorial, para lo cual deben dar debido cumplimiento a los deberes de recíproca información y de colaboración y cooperación mutuas en el ejercicio de sus actuaciones y de sus competencias.

En defecto de acuerdo entre las Administraciones públicas, cuando quede plenamente justificada la necesidad de redes públicas de comunicaciones electrónicas, y siempre y cuando se cumplan los parámetros y requerimientos técnicos esenciales para garantizar el funcionamiento de las redes y servicios de comunicaciones electrónicas establecidos en el apartado 5 del artículo 49, el Consejo de Ministros podrá autorizar la ubicación o el itinerario concreto de una infraestructura de red de comunicaciones electrónicas, en cuyo caso la Administración Pública competente deberá incorporar necesariamente en sus respectivos instrumentos de ordenación las rectificaciones imprescindibles para acomodar sus determinaciones a aquéllas, salvo que esté plenamente justificada su imposibilidad por razones de medio ambiente u ordenación urbana y territorial, o por su ubicación en edificaciones afectas a las Fuerzas y Cuerpos de Seguridad, en cuyo caso deberá ir acompañado de las alternativas oportunas, factibles y viables que permitan el despliegue efectivo de la red y garantizar en la práctica el derecho de ocupación de los operadores y su ejercicio en igualdad de condiciones.

5. La tramitación por la Administración Pública competente de una medida cautelar que impida o paralice o de una resolución que deniegue o imposibilite la instalación de la infraestructura de red o recursos asociados que cumpla los parámetros y requerimientos técnicos esenciales para garantizar el funcionamiento de las distintas redes y servicios de comunicaciones electrónicas establecidos en el apartado 5 del artículo 49, excepto en edificaciones del patrimonio histórico-artístico con la categoría de bien de interés cultural, será objeto de previo informe preceptivo del Ministerio de Asuntos Económicos y Transformación Digital, que dispone del plazo máximo de un mes para su emisión y que será evacuado tras, en su caso, los intentos que procedan de encontrar una solución negociada con los órganos encargados de la tramitación de la citada medida o resolución.

Sin perjuicio de lo dispuesto en el artículo 80.4 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, transcurrido dicho

plazo, el informe se entenderá emitido con carácter favorable y podrá continuarse con la tramitación de la medida o resolución.

A falta de solicitud del preceptivo informe, así como en el supuesto de que el informe no sea favorable, no se podrá aprobar la medida o resolución.

6. El Ministerio de Asuntos Económicos y Transformación Digital promoverá con la asociación de entidades locales de ámbito estatal con mayor implantación la elaboración de un modelo tipo de declaración responsable a que se refiere el apartado 9 del artículo 49.

7. Igualmente, el Ministerio de Asuntos Económicos y Transformación Digital aprobará recomendaciones para la elaboración por parte de las Administraciones públicas competentes de las normas o instrumentos contemplados en la presente sección, que podrán contener modelos de ordenanzas municipales elaborados conjuntamente con la asociación de entidades locales de ámbito estatal con mayor implantación. En el caso de municipios se podrá reemplazar la solicitud de informe a que se refiere el apartado 2 de este artículo por la presentación al Ministerio de Asuntos Económicos y Transformación Digital del proyecto de instrumento acompañado de la declaración del Alcalde del municipio acreditando el cumplimiento de dichas recomendaciones.

8. El Ministerio de Asuntos Económicos y Transformación Digital creará un punto de gestión único a través del cual los operadores de redes públicas de comunicaciones electrónicas y de servicios de comunicaciones electrónicas disponibles al público accederán por vía electrónica a toda la información relativa sobre las condiciones y procedimientos aplicables para la instalación y despliegue de redes de comunicaciones electrónicas y sus recursos asociados, así como a la información para el cumplimiento de las obligaciones tributarias específicas de ámbito autonómico y local, a través de los enlaces de las administraciones correspondientes.

Las Comunidades Autónomas y las Corporaciones Locales podrán, mediante la suscripción del oportuno convenio de colaboración con el Ministerio de Asuntos Económicos y Transformación Digital, adherirse al punto de gestión único, en cuyo caso, los operadores de comunicaciones electrónicas deberán presentar en formato electrónico a través de dicho punto las declaraciones responsables a que se refiere el apartado 5 del artículo 49 y permisos de toda índole para el despliegue de dichas redes que vayan dirigidas a la respectiva Comunidad Autónoma o Corporación Local. En el ámbito tributario, el punto de gestión único permitirá la conexión con la sede electrónica de dichas Administraciones, al objeto de que se pueda disponer de información de manera centralizada, más simplificada, accesible y eficiente, por parte de los operadores de redes públicas de comunicaciones electrónicas y de servicios de comunicaciones electrónicas disponibles al público, facilitando el cumplimiento de las obligaciones tributarias específicas en los ámbitos autonómico y local, sin perjuicio de las competencias que, en el ámbito de aplicación de los tributos, corresponden a las citadas administraciones.

El punto de gestión único será gestionado por el Ministerio de Asuntos Económicos y Transformación Digital y será el encargado de remitir a la Comunidad Autónoma o Corporación Local que se haya adherido a dicho punto todas las declaraciones responsables y solicitudes para la instalación y despliegue de redes de comunicaciones electrónicas y sus recursos asociados que les hayan presentado los operadores de redes públicas de comunicaciones electrónicas.

El Ministerio de Asuntos Económicos y Transformación Digital, las Comunidades Autónomas y la asociación de entidades locales de ámbito estatal con mayor implantación fomentarán el uso de este punto de gestión único por el conjunto de las Administraciones públicas con vistas a reducir cargas y costes administrativos, facilitar la interlocución de los operadores con la Administración y simplificar el cumplimiento de los trámites administrativos.

Artículo 51. *Previsión de infraestructuras de comunicaciones electrónicas en proyectos de urbanización y en obras civiles financiadas con recursos públicos.*

1. Cuando se acometan proyectos de urbanización, el proyecto técnico de urbanización deberá ir acompañado de un proyecto específico de telecomunicaciones que deberá prever la instalación de infraestructura de obra civil para facilitar la instalación y explotación de las redes públicas de comunicaciones electrónicas, pudiendo incluir adicionalmente elementos y

equipos de red pasivos en los términos que determine la normativa técnica de telecomunicaciones que se dicte en desarrollo de este artículo.

Las infraestructuras que se instalen para facilitar la instalación y explotación de las redes públicas de comunicaciones electrónicas conforme al párrafo anterior formarán parte del conjunto resultante de las obras de urbanización y pasarán a integrarse en el dominio público municipal. La Administración Pública titular de dicho dominio público pondrá tales infraestructuras a disposición de los operadores interesados en condiciones de igualdad, transparencia y no discriminación.

Mediante real decreto se establecerá el dimensionamiento y características técnicas mínimas que habrán de reunir estas infraestructuras.

2. En las obras civiles financiadas total o parcialmente con recursos públicos se preverá, en los supuestos y condiciones que se determinen mediante real decreto, la instalación de recursos asociados y otras infraestructuras de obra civil para facilitar el despliegue de las redes públicas de comunicaciones electrónicas, que se pondrán a disposición de los operadores interesados en condiciones de igualdad, transparencia y no discriminación.

Sección 3.ª Acceso a infraestructuras susceptibles de alojar redes públicas de comunicaciones electrónicas y coordinación de obras civiles

Artículo 52. *Acceso a las infraestructuras susceptibles de alojar redes públicas de comunicaciones electrónicas.*

1. Los operadores de redes públicas de comunicaciones electrónicas podrán acceder a las infraestructuras susceptibles de alojar redes públicas de comunicaciones electrónicas para la instalación o explotación de redes de alta y muy alta capacidad, en los términos indicados en el presente artículo.

2. Cuando un operador que instale o explote redes públicas de comunicaciones electrónicas realice una solicitud razonable de acceso a una infraestructura física a alguno de los sujetos obligados, éste estará obligado a atender y negociar dicha solicitud de acceso, en condiciones equitativas y razonables, en particular, en cuanto al precio, con vistas al despliegue de elementos de las redes de comunicaciones electrónicas de alta y muy alta capacidad.

No se estará obligado a negociar el acceso en relación con aquellas infraestructuras vinculadas con la seguridad nacional, la defensa nacional o la seguridad pública, o cuando tengan la consideración de críticas en virtud de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. En este último caso, para la negociación del acceso a dichas infraestructuras será preceptivo el informe de la Secretaría de Estado de Seguridad del Ministerio del Interior.

3. Son sujetos obligados los siguientes propietarios, gestores o titulares de derechos de utilización de infraestructuras físicas susceptibles de alojar redes públicas de comunicaciones electrónicas de alta o muy alta capacidad:

a) operadores de redes que proporcionen una infraestructura física destinada a prestar un servicio de producción, transporte o distribución de:

1.º gas;

2.º electricidad, incluida la iluminación pública;

3.º calefacción;

4.º agua, incluidos los sistemas de saneamiento: evacuación o tratamiento de aguas residuales y el alcantarillado y los sistemas de drenaje. No se incluye dentro de esta definición a los elementos de redes utilizados para el transporte de agua destinada al consumo humano, definida esta última según lo establecido en el Real Decreto 140/2003, de 7 de febrero, por el que se establecen los criterios sanitarios de la calidad del agua de consumo humano;

b) operadores que instalen o exploten redes públicas de comunicaciones electrónicas disponibles para el público;

c) empresas que proporcionen infraestructuras físicas destinadas a prestar servicios de transporte, incluidos los ferrocarriles, las carreteras, los puertos y los aeropuertos,

incluyendo a las entidades o sociedades encargadas de la gestión de infraestructuras de transporte de competencia estatal;

d) las Administraciones públicas titulares de infraestructuras físicas susceptibles de alojar redes públicas de comunicaciones electrónicas.

Los sujetos obligados deberán atender y negociar las solicitudes de acceso a su infraestructura física al objeto de facilitar el despliegue de redes de comunicaciones electrónicas de alta o muy alta capacidad. En los casos en que la solicitud de acceso se produzca sobre una infraestructura gestionada o cuya titularidad o derecho de uso corresponda a un operador de comunicaciones electrónicas sujeto a obligaciones motivadas por los artículos 17 y 18, el acceso a dichas infraestructuras físicas será coherente con tales obligaciones y la introducción de procedimientos y tareas nuevas se basará en las ya existentes.

4. Por infraestructuras susceptibles de ser utilizadas para el despliegue de redes públicas de comunicaciones electrónicas de alta o muy alta capacidad se entiende cualquier elemento de una red pensado para albergar otros elementos de una red sin llegar a ser un elemento activo de ella, como tuberías, mástiles, conductos, cámaras de acceso, bocas de inspección, distribuidores, edificios o entradas a edificios, instalaciones de antenas, torres y postes. Los cables, incluida la fibra oscura, así como los elementos de redes utilizados para el transporte de agua destinada al consumo humano, no son infraestructura física en el sentido de este artículo.

5. En particular, se garantiza que los operadores de redes públicas de comunicaciones electrónicas tengan derecho a acceder, en los términos establecidos en la normativa europea, a cualquier infraestructura física controlada por las Administraciones públicas que sea técnicamente apta para acoger puntos de acceso inalámbrico para pequeñas áreas o que sea necesaria para conectar dichos puntos de acceso a una red troncal, en particular mobiliario urbano, como postes de luz, señales viales, semáforos, vallas publicitarias, paradas de autobús y de tranvía y estaciones de metro. Las autoridades públicas satisfarán todas las solicitudes razonables de acceso en el marco de unas condiciones justas, razonables, transparentes y no discriminatorias, que serán hechas públicas en el punto de información único a que se refiere el apartado 13 de este artículo.

6. El acceso a dichas infraestructuras para la instalación o explotación de una red no podrá ser otorgado o reconocido mediante procedimientos de licitación.

Las Administraciones públicas titulares de las infraestructuras a las que se hace referencia en este artículo tendrán derecho a establecer las compensaciones económicas que correspondan por el uso que de ellas se haga por parte de los operadores.

7. Cualquier denegación de acceso deberá justificarse de manera clara al solicitante, en el plazo máximo de dos meses a partir de la fecha de recepción de la solicitud de acceso completa, exponiendo los motivos en los que se fundamenta. La denegación deberá basarse en criterios objetivos, transparentes y proporcionados, tales como:

a) la falta de idoneidad técnica de la infraestructura física a la que se ha solicitado acceso para albergar cualquiera de los elementos de las redes de comunicaciones electrónicas de alta y muy alta capacidad. Los motivos de denegación basados en la falta de adecuación técnica de la infraestructura serán determinadas por el Ministerio de Asuntos Económicos y Transformación Digital mediante orden, previo informe del departamento ministerial con competencia sectorial sobre dicha infraestructura;

b) la falta de disponibilidad de espacio para acoger los elementos de las redes de comunicaciones electrónicas de alta y muy alta capacidad, incluidas las futuras necesidades de espacio del sujeto obligado, siempre y cuando esto quede suficientemente demostrado;

c) los riesgos para la seguridad nacional, la defensa nacional, la seguridad pública, la salud pública, la seguridad vial o la protección civil;

d) los riesgos para la integridad y la seguridad de una red, en particular de las infraestructuras nacionales críticas, sin perjuicio de lo dispuesto en el apartado 2 de este artículo;

e) los riesgos de interferencias graves de los servicios de comunicaciones electrónicas previstos con la prestación de otros servicios a través de la misma infraestructura física;

f) la disponibilidad de medios alternativos viables de acceso a la infraestructura de red física al por mayor facilitados por el sujeto obligado y que sean adecuados para el suministro de redes de comunicaciones electrónicas de alta y muy alta capacidad, siempre que dicho acceso se ofrezca en condiciones justas y razonables;

g) garantizar que no se comprometa la continuidad y seguridad de la prestación de los servicios públicos o de carácter público que en dichas infraestructuras realiza su Administración Pública titular.

8. Cualquiera de las partes podrá plantear un conflicto ante la Comisión Nacional de los Mercados y la Competencia cuando se deniegue el acceso o cuando transcurrido el plazo de dos meses mencionado en el apartado anterior, no se llegue a un acuerdo sobre las condiciones en las que debe producirse el mismo, incluidos los precios. La Comisión Nacional de los Mercados y la Competencia, teniendo plenamente en cuenta el principio de proporcionalidad, adoptará, en el plazo máximo de cuatro meses desde la recepción de toda la información, una decisión para resolverlo, incluida la fijación de condiciones y precios equitativos y no discriminatorios cuando proceda.

9. A fin de solicitar el acceso a una infraestructura física de conformidad con lo dispuesto en este artículo, los operadores que instalen o exploten redes públicas de comunicaciones electrónicas tienen derecho a acceder, previa solicitud por escrito en la que se especifique la zona en la que tienen intención de desplegar elementos de las redes de comunicaciones electrónicas de alta y muy alta capacidad a la siguiente información mínima relativa a las infraestructuras físicas existentes de cualquiera de los sujetos obligados:

a) localización y trazado de la infraestructura;

b) tipo y utilización de la misma, describiendo su grado de ocupación actual;

c) punto de contacto al que dirigirse.

10. Los sujetos obligados tienen la obligación de atender las solicitudes de información mínima relativa a las infraestructuras físicas susceptibles de alojar redes de comunicaciones electrónicas, otorgando el acceso a dicha información en condiciones proporcionadas, no discriminatorias y transparentes, en el plazo de dos meses a partir de la fecha de recepción de la solicitud.

Asimismo, los sujetos obligados tienen la obligación de atender las solicitudes razonables de realización de estudios sobre el terreno de elementos específicos de sus infraestructuras físicas susceptibles de alojar redes de comunicaciones electrónicas.

El acceso a la información mínima podrá estar limitado si es necesario por motivos de seguridad e integridad de las redes, de seguridad y defensa nacional, de salud o seguridad pública, en el caso de infraestructuras críticas o por motivos de confidencialidad o de secreto comercial u operativo.

11. Las solicitudes de información mínima y las solicitudes de estudios sobre el terreno podrán ser denegadas de manera justificada, en el caso de infraestructuras nacionales críticas o de infraestructuras que no se consideren técnicamente adecuadas para el despliegue de redes de comunicaciones electrónicas de alta y muy alta capacidad, así como por motivos de seguridad nacional, defensa nacional, seguridad y salud pública.

12. Cualquiera de las partes podrá plantear los conflictos que pudieran surgir en relación con las solicitudes de información mínima y las solicitudes de estudios sobre el terreno, ante la Comisión Nacional de los Mercados y la Competencia quien, teniendo plenamente en cuenta el principio de proporcionalidad, resolverá la diferencia en un plazo máximo de dos meses desde la recepción de toda la información.

13. El Ministerio de Asuntos Económicos y Transformación Digital gestionará a través del punto de información único la información en materia de infraestructuras existentes. Mediante el punto de información único los sujetos obligados podrán poner a disposición de los operadores que instalen o exploten redes públicas de comunicaciones electrónicas, información relativa a sus infraestructuras susceptibles de alojar redes de comunicaciones electrónicas de alta y muy alta capacidad en particular, su ubicación detallada.

14. Mediante real decreto se desarrollará lo establecido en este artículo, atendiendo a lo dispuesto en la Directiva 2014/61/UE, del Parlamento Europeo y del Consejo, de 15 de mayo de 2014, relativa a medidas para reducir el coste del despliegue de las redes de comunicaciones electrónicas de alta velocidad.

15. Lo previsto en este artículo se entenderá sin perjuicio de lo dispuesto en la normativa de defensa de la competencia. Los operadores que suministren redes de comunicaciones electrónicas que obtengan acceso a información en virtud del presente artículo adoptarán las medidas adecuadas para garantizar el respeto de la confidencialidad y el secreto comercial u operativo.

Artículo 53. *Coordinación de obras civiles.*

1. Todo sujeto obligado, en los términos indicados en el artículo 52, tendrá derecho a negociar acuerdos relativos a la coordinación de obras civiles con operadores que instalen o exploten redes públicas de comunicaciones electrónicas, con vistas al despliegue de elementos de las redes de comunicaciones electrónicas de alta y muy alta capacidad.

2. Los sujetos obligados que realicen directa o indirectamente obras civiles, total o parcialmente financiadas con recursos públicos deberán atender y negociar las solicitudes de coordinación de dichas obras civiles, al objeto de facilitar el despliegue de redes de comunicaciones electrónicas de alta y muy alta capacidad.

3. A tal fin, cuando un operador que instale o explote redes públicas de comunicaciones electrónicas disponibles al público realice una solicitud razonable de coordinación de las obras a las que se refiere el apartado anterior con vistas al despliegue de elementos de las redes de comunicaciones electrónicas de alta y muy alta capacidad, los sujetos obligados atenderán dicha solicitud en condiciones transparentes y no discriminatorias.

4. Las obligaciones establecidas en el presente artículo no se aplicarán en relación con las infraestructuras nacionales críticas y con las obras civiles de importancia insignificante.

5. Cuando en el plazo de un mes a partir de la fecha de recepción de la solicitud formal de coordinación de obras civiles no se haya conseguido un acuerdo, cualquiera de las partes, sin perjuicio del sometimiento de la cuestión a los tribunales, podrá plantear el conflicto ante la Comisión Nacional de los Mercados y la Competencia. La Comisión Nacional de los Mercados y la Competencia, teniendo plenamente en cuenta el principio de proporcionalidad, adoptará, en el plazo máximo de dos meses desde la recepción de toda la información, una decisión para resolver el conflicto, incluida la fijación de condiciones y precios equitativos y no discriminatorios cuando proceda.

6. A fin de negociar los acuerdos relativos a la coordinación de obras civiles a que hace referencia este artículo, los operadores que instalen o exploten redes públicas de comunicaciones electrónicas tienen derecho a acceder, previa solicitud por escrito, en la que se especifique la zona en la que tienen intención de desplegar elementos de las redes de comunicaciones electrónicas de alta y muy alta capacidad, a la siguiente información mínima relativa a las obras civiles relacionadas con la infraestructura física de los sujetos obligados, que estén en curso, para las que se haya presentado solicitud de permiso y aún no haya sido concedido o para las que se prevea realizar la primera presentación de solicitud de permiso, licencia o de la documentación que la sustituya ante las autoridades competentes en los seis meses siguientes a la presentación de la solicitud de coordinación:

a) localización y tipo de obra;
b) elementos de la red implicados;
c) fecha prevista de inicio de las obras y duración de estas, y
d) punto de contacto al que dirigirse.

7. Los sujetos obligados tienen la obligación de atender las solicitudes de información mínima relativa a las obras civiles en curso o previstas, otorgando el acceso a dicha información, en condiciones proporcionadas, no discriminatorias y transparentes, en el plazo de dos semanas a partir de la fecha de recepción de la solicitud.

8. Los sujetos obligados podrán limitar el acceso a la información mínima si es necesario por motivos de seguridad e integridad de las redes, de seguridad y defensa nacional, de salud o seguridad pública, de confidencialidad o de secreto comercial u operativo.

9. Cualquiera de las partes podrá plantear los conflictos que pudieran surgir en relación con las solicitudes de información mínima relativa a las obras civiles, ante la Comisión Nacional de los Mercados y la Competencia quien, teniendo plenamente en cuenta el principio de proporcionalidad, resolverá la diferencia en un plazo máximo de dos meses desde la recepción de toda la información.

10. El Ministerio de Asuntos Económicos y Transformación Digital gestionará el punto de información único de coordinación de obras civiles a través del cual los operadores que instalen o exploten redes públicas de comunicaciones electrónicas podrán acceder a la información mínima contemplada en este artículo.

11. Mediante real decreto se desarrollará lo establecido en este artículo, atendiendo a lo dispuesto en la Directiva 2014/61/UE, del Parlamento Europeo y del Consejo, de 15 de mayo de 2014, relativa a medidas para reducir el coste del despliegue de las redes de comunicaciones electrónicas de alta velocidad.

12. Lo establecido en el presente artículo se entenderá sin perjuicio de lo dispuesto en el artículo 51.2 o de cualquier obligación de reservar capacidad para el despliegue de redes públicas de comunicaciones electrónicas, independientemente de la existencia o no de solicitudes de coordinación de obra civil y sin perjuicio asimismo de lo dispuesto en la normativa de defensa de la competencia.

Artículo 54. *Acceso o uso de las redes de comunicaciones electrónicas titularidad de los órganos o entes gestores de infraestructuras de transporte de competencia estatal.*

1. Los órganos o entes pertenecientes a la Administración General del Estado así como cualesquiera otras entidades o sociedades encargados de la gestión de infraestructuras de transporte de competencia estatal que presten, directamente o a través de entidades o sociedades intermedias, servicios de comunicaciones electrónicas o comercialicen la explotación de redes públicas de comunicaciones electrónicas, negociarán con los operadores de redes y servicios de comunicaciones electrónicas interesados en el acceso o uso de las redes de comunicaciones electrónicas de las que aquellos sean titulares.

2. Las condiciones para el acceso o uso de estas redes han de ser equitativas, no discriminatorias, objetivas, transparentes, neutrales y a precios de mercado, siempre que se garantice al menos la recuperación de coste de las inversiones y su operación y mantenimiento, para todos los operadores de redes y servicios de comunicaciones electrónicas, incluidos los pertenecientes o vinculados a dichos órganos o entes, sin que en ningún caso pueda establecerse derecho preferente o exclusivo alguno de acceso o uso a dichas redes en beneficio de un operador determinado o de una red concreta de comunicaciones electrónicas. En todo caso, deberá preservarse la seguridad de las infraestructuras de transporte en las que están instaladas las redes de comunicaciones electrónicas a que se refiere este artículo y de los servicios que en dichas infraestructuras se prestan.

3. Las partes acordarán libremente los acuerdos del acceso o uso a que se refiere este artículo, a partir de las condiciones establecidas en el apartado anterior y sin perjuicio asimismo de lo dispuesto en la normativa de defensa de la competencia. Cualquiera de las partes podrá presentar un conflicto sobre el acceso y sus condiciones ante la Comisión Nacional de los Mercados y la Competencia, la cual, previa audiencia de las partes, dictará resolución vinculante sobre los extremos objeto del conflicto, en el plazo de cuatro meses, sin perjuicio de que puedan adoptarse medidas provisionales hasta el momento en que se dicte la resolución definitiva.

Sección 4.ª Infraestructuras comunes y redes de comunicaciones electrónicas en los edificios

Artículo 55. *Infraestructuras comunes y redes de comunicaciones electrónicas en los edificios.*

1. Mediante real decreto se desarrollará la normativa legal en materia de infraestructuras comunes de comunicaciones electrónicas en el interior de edificios y conjuntos inmobiliarios. Dicho real decreto determinará, tanto el punto de interconexión de la red interior con las redes públicas, como las condiciones aplicables a la propia red interior. Asimismo, regulará las garantías aplicables al acceso a los servicios de comunicaciones electrónicas a través de sistemas individuales en defecto de infraestructuras comunes de comunicaciones electrónicas, y el régimen de instalación de éstas en todos aquellos aspectos no previstos en las disposiciones con rango legal reguladoras de la materia.

2. La normativa técnica básica de edificación que regule la infraestructura de obra civil en el interior de los edificios y conjuntos inmobiliarios deberá tomar en consideración las necesidades de soporte de los sistemas y redes de comunicaciones electrónicas fijadas de conformidad con la normativa a que se refiere el apartado 1, previendo que la infraestructura de obra civil disponga de capacidad suficiente para permitir el paso de las redes de los distintos operadores, de forma que se facilite la posibilidad de uso compartido de estas infraestructuras por aquéllos.

3. La normativa reguladora de las infraestructuras comunes de comunicaciones electrónicas promoverá la sostenibilidad de las edificaciones y conjuntos inmobiliarios, de uso residencial, industrial, terciario y dotacional, facilitando la introducción de aquellas tecnologías de la información y las comunicaciones y el «Internet de las Cosas» que favorezcan su eficiencia energética, accesibilidad y seguridad, tendiendo hacia la implantación progresiva en España del edificio sostenible y conectado con unidades de convivencia superiores y del concepto de hogar digital.

4. El Ministerio de Asuntos Económicos y Transformación Digital creará y mantendrá un inventario centralizado y actualizado de todos aquellos edificios o conjuntos inmobiliarios que disponen de infraestructuras comunes de telecomunicaciones instaladas. Dicho inventario será puesto a disposición de los operadores y de las empresas instaladoras de telecomunicación.

5. Los operadores podrán instalar los tramos finales de las redes fijas de comunicaciones electrónicas de alta y muy alta capacidad así como sus recursos asociados en los edificios, fincas y conjuntos inmobiliarios que estén acogidos, o deban acogerse, al régimen de propiedad horizontal o a los edificios que, en todo o en parte, hayan sido o sean objeto de arrendamiento por plazo superior a un año, salvo los que alberguen una sola vivienda, al objeto de que cualquier copropietario o, en su caso, arrendatario del inmueble pueda hacer uso de dichas redes.

En el caso de edificios en los que no exista una infraestructura común de comunicaciones electrónicas en el interior del edificio o conjunto inmobiliario, o la existente no permita instalar el correspondiente acceso a las redes fijas de comunicaciones electrónicas de alta y muy alta capacidad, dicha instalación podrá realizarse haciendo uso de los elementos comunes de la edificación. En los casos en los que no sea posible realizar la instalación en el interior de la edificación o finca por razones técnicas o económicas, la instalación podrá realizarse utilizando las fachadas de las edificaciones.

El operador que se proponga instalar los tramos finales de red y sus recursos asociados a que se refiere el presente apartado, deberá comunicarlo por escrito a la comunidad de propietarios o, en su caso, al propietario del edificio, junto con una descripción de la actuación que pretende realizar, antes de iniciar cualquier instalación. El formato, contenido, y plazos formales de presentación tanto de la comunicación escrita como de la descripción de actuación referidos en el presente párrafo serán determinados reglamentariamente. En todo caso, corresponderá al operador acreditar que la comunicación escrita ha sido entregada.

La instalación no podrá realizarse si en el plazo de un mes desde que la comunicación se produzca, la comunidad de propietarios o el propietario acredita ante el operador que ninguno de los copropietarios o arrendatarios del edificio está interesado en disponer de las infraestructuras propuestas, o afirma que va a realizar, dentro de los tres meses siguientes a la contestación, la instalación de una infraestructura común de comunicaciones electrónicas en el interior del edificio o la adaptación de la previamente existente que permita dicho acceso de alta o muy alta capacidad. Transcurrido el plazo de un mes antes señalado desde que la comunicación se produzca sin que el operador hubiera obtenido respuesta, o el plazo de tres meses siguientes a la contestación sin que se haya realizado la instalación de la infraestructura común de comunicaciones electrónicas, el operador estará habilitado para iniciar la instalación de los tramos finales de red y sus recursos asociados, si bien será necesario que el operador indique a la comunidad de propietarios o al propietario el día de inicio de la instalación.

El procedimiento del párrafo anterior no será aplicable al operador que se proponga instalar los tramos finales de redes fijas de comunicaciones electrónicas de alta y muy alta capacidad y sus recursos asociados en un edificio o conjunto inmobiliario en el que otro

operador haya iniciado o instalado tramos finales de dichas redes; o en aquellos casos, sean edificaciones o fincas sujetas al régimen de propiedad horizontal o no, en los que se trate de un tramo para dar continuidad a una instalación que sea necesaria para proporcionar acceso a dichas redes en edificios o fincas colindantes o cercanas y no exista otra alternativa económicamente eficiente y técnicamente viable que quede justificada, en cuyo caso la comunidad de propietarios o el propietario no podrá denegar al operador la instalación de los tramos finales en el edificio, ni podrá denegar la instalación del tramo de red necesario para dar continuidad de la red hacia los edificios o fincas colindantes. En ambos supuestos deberá existir, en todo caso, una comunicación previa mínima de un mes de antelación del operador a la comunidad de propietarios o al propietario junto con una descripción de la actuación que pretende realizar, antes de iniciar cualquier instalación.

En todo caso, será necesario que el operador indique a la comunidad de propietarios o al propietario el día de inicio de la instalación.

6. Los operadores serán responsables de cualquier daño que inflijan en las edificaciones o fincas como consecuencia de las actividades de instalación de las redes y recursos asociados a que se refiere el apartado anterior.

7. Por orden del Ministerio de Asuntos Económicos y Transformación Digital se determinarán los aspectos técnicos que deben cumplir los operadores en la instalación de los recursos asociados a las redes fijas de comunicaciones electrónicas de alta y muy alta capacidad así como la obra civil asociada en los supuestos contemplados en el apartado 5 de este artículo, con el objetivo de reducir molestias y cargas a los ciudadanos, optimizar la instalación de las redes y facilitar el despliegue de las redes por los distintos operadores.

8. La Comisión Nacional de los Mercados y la Competencia podrá imponer, previa solicitud razonable o de oficio, a los operadores y a los propietarios de los correspondientes cables o recursos asociados cuando estos propietarios no sean operadores, previo trámite de información pública, obligaciones objetivas, transparentes, proporcionadas y no discriminatorias relativas al acceso o utilización compartida de los tramos finales de las redes de acceso, incluyendo los que discurran por el interior de las edificaciones y conjuntos inmobiliarios, o hasta el primer punto de concentración o distribución ubicado en su exterior, cuando la duplicación de esta infraestructura sea económicamente ineficiente o físicamente inviable. Las condiciones impuestas podrán incluir normas específicas sobre el acceso a dichos elementos de redes y a los recursos y servicios asociados, transparencia y no discriminación, así como de prorrateo de los costes de acceso, los cuales, en su caso, se ajustarán para tener en cuenta los factores de riesgo.

Cuando la Comisión Nacional de los Mercados y la Competencia concluya, habida cuenta en su caso de las obligaciones resultantes de cualquier análisis de mercado pertinente, que las obligaciones impuestas en virtud de lo dispuesto en el párrafo anterior no resuelven de modo suficiente barreras físicas o económicas importantes y no transitorias a la replicación subyacente a una situación existente o incipiente en el mercado que limitan significativamente los resultados de competitividad para los usuarios finales, podrá ampliar la imposición de dichas obligaciones de acceso, en condiciones justas y razonables, más allá del primer punto de concentración o distribución hasta un punto que considere es el más próximo a los usuarios finales que pueda acoger un número de conexiones de usuarios finales suficiente como para ser viable comercialmente para los solicitantes de acceso eficientes. Al determinar la extensión de la ampliación más allá del primer punto de concentración o de distribución, la Comisión Nacional de los Mercados y la Competencia tendrá en cuenta en la mayor medida posible las correspondientes directrices del ORECE. Si ello se justifica por motivos técnicos o económicos, la Comisión Nacional de los Mercados y la Competencia podrá imponer unas obligaciones de acceso activas o virtuales.

La Comisión Nacional de los Mercados y la Competencia no impondrá las obligaciones mencionadas en el párrafo anterior en cualquiera de los siguientes supuestos:

a) el operador sea exclusivamente mayorista y pone a disposición de cualquier operador unos medios de acceso a los usuarios finales alternativos, viables y similares en condiciones justas, no discriminatorias y razonables a una red de muy alta capacidad. La Comisión Nacional de los Mercados y la Competencia podrá hacer extensiva esta exención a otros operadores que ofrezcan, en condiciones justas, no discriminatorias y razonables, acceso a

una red de muy alta capacidad. Esta exención no podrá aplicarse cuando las redes públicas de comunicaciones electrónicas sean o hayan sido financiadas públicamente;

b) se ponga en peligro la viabilidad económica o financiera de un nuevo despliegue de redes, en particular mediante proyectos locales de menor dimensión.

CAPÍTULO III

Salvaguardia de derechos fundamentales, secreto de las comunicaciones y protección de los datos personales y derechos y obligaciones de carácter público vinculados con las redes y servicios de comunicaciones electrónicas

Artículo 56. *Salvaguardia de derechos fundamentales.*

1. Las medidas que se adopten en relación al acceso o al uso por parte de los usuarios finales de los servicios y las aplicaciones a través de redes de comunicaciones electrónicas respetarán los derechos y libertades fundamentales, como queda garantizado en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, en la Carta de Derechos Fundamentales de la Unión Europea, en los principios generales del Derecho comunitario y en la Constitución Española.

2. Cualquiera de esas medidas relativas al acceso o al uso por parte de los usuarios finales de los servicios y las aplicaciones a través de redes de comunicaciones electrónicas, que sea susceptible de restringir esos derechos y libertades fundamentales solo podrá imponerse si es adecuada, necesaria y proporcionada en una sociedad democrática, y su aplicación está sujeta a las salvaguardias de procedimiento apropiadas de conformidad con las normas mencionadas en el apartado anterior. Por tanto, dichas medidas solo podrán ser adoptadas respetando debidamente el principio de presunción de inocencia, el derecho a la vida privada e intimidad, el derecho a la libertad de expresión e información y el derecho a la tutela judicial efectiva, a través de un procedimiento previo, justo e imparcial, que incluirá el derecho de los interesados a ser oídos, sin perjuicio de que concurran las condiciones y los requisitos procedimentales adecuados en los casos de urgencia debidamente justificados, de conformidad con el Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales y la Carta de los Derechos Fundamentales de la Unión Europea.

Artículo 57. *Principio de no discriminación.*

Los operadores que instalen o exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público no aplicarán a los usuarios finales ningún requisito diferente ni condiciones generales de acceso o uso de redes o servicios ni de utilización de los mismos por motivos relacionados con la nacionalidad, el lugar de residencia o el lugar de establecimiento del usuario final, a menos que dicho trato diferente se justifique de forma objetiva.

Artículo 58. *Secreto de las comunicaciones.*

1. Los operadores que suministren redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público deberán garantizar el secreto de las comunicaciones de conformidad con los artículos 18.3 y 55.2 de la Constitución, debiendo adoptar las medidas técnicas necesarias.

2. Los operadores que suministren redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones interpersonales basados en numeración disponibles al público o servicios de acceso a internet están obligados a realizar las interceptaciones que se autoricen judicialmente de acuerdo con lo establecido en el capítulo V del título VIII del libro II de la Ley de Enjuiciamiento Criminal, en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia y en otras normas con rango de ley orgánica. Asimismo, deberán adoptar a su costa las medidas que se establecen en este artículo y en los reglamentos correspondientes.

3. La interceptación a que se refiere el apartado anterior deberá facilitarse para cualquier comunicación que tenga como origen o destino el punto de terminación de red o el terminal específico que se determine a partir de la orden de interceptación legal, incluso aunque esté

destinada a dispositivo de almacenamiento o procesamiento de la información; asimismo, la interceptación podrá realizarse sobre un terminal conocido y con unos datos de ubicación temporal para comunicaciones desde locales públicos. Cuando no exista una vinculación fija entre el sujeto de la interceptación y el terminal utilizado, éste podrá ser determinado dinámicamente cuando el sujeto de la interceptación lo active para la comunicación mediante un código de identificación personal.

4. El acceso se facilitará para todo tipo de comunicaciones electrónicas disponibles al público distintas de las comunicaciones interpersonales independientes de la numeración, en particular, por su penetración y cobertura, para las que se realicen mediante cualquier modalidad de los servicios de telefonía y de transmisión de datos, se trate de comunicaciones de vídeo, audio, intercambio de mensajes, ficheros o de la transmisión de facsímiles.

El acceso facilitado servirá tanto para la supervisión como para la transmisión a los centros de recepción de las interceptaciones de la comunicación electrónica interceptada y la información relativa a la interceptación, y permitirá obtener la señal con la que se realiza la comunicación.

5. Los sujetos obligados deberán facilitar al agente facultado, salvo que por las características del servicio no estén a su disposición, los datos indicados en la orden de interceptación legal, de entre los que se relacionan a continuación:

a) identidad o identidades del sujeto objeto de la medida de la interceptación.

Se entiende por identidad: etiqueta técnica que puede representar el origen o el destino de cualquier tráfico de comunicaciones electrónicas, en general identificada mediante un número de identidad de comunicaciones electrónicas físico (tal como un número de teléfono) o un código de identidad de comunicaciones electrónicas lógico o virtual (tal como un número personal) que el abonado puede asignar a un acceso físico caso a caso.

Los sujetos obligados proporcionarán, cuando técnicamente sea posible, los identificadores permanentes que sean necesarios para la atribución de un servicio a un usuario determinado de forma inequívoca, así como los identificadores del dispositivo empleado para la comunicación.

Si en una comunicación electrónica se asignaran identidades de carácter temporal al usuario, el sujeto obligado implementará, cuando técnicamente sea posible, las medidas de correlación necesarias para que en la información de la interceptación se faciliten las identidades permanentes que permitan la identificación inequívoca del usuario asignado, así como del dispositivo empleado en la comunicación.

b) identidad o identidades de las otras partes involucradas en la comunicación electrónica;

c) servicios básicos utilizados;

d) servicios suplementarios utilizados;

e) dirección de la comunicación;

f) indicación de respuesta;

g) causa de finalización;

h) marcas temporales;

i) información de localización;

j) información intercambiada a través del canal de control o señalización.

6. Además de la información relativa a la interceptación prevista en el apartado anterior, los sujetos obligados deberán facilitar al agente facultado, salvo que por las características del servicio no estén a su disposición, de cualquiera de las partes que intervengan en la comunicación que sean clientes del sujeto obligado, los siguientes datos:

a) identificación de la persona física o jurídica;

b) domicilio en el que el operador realiza las notificaciones;

y, aunque no sea abonado, si el servicio de que se trata permite disponer de alguno de los siguientes:

c) número de titular de servicio (tanto el número de directorio como todas las identificaciones de comunicaciones electrónicas del abonado);

d) número de identificación del terminal;

e) número de cuenta asignada por el proveedor de servicios internet;
f) dirección de correo electrónico.

7. Junto con los datos previstos en los apartados anteriores, los sujetos obligados deberán facilitar, salvo que por las características del servicio no esté a su disposición, información de la situación geográfica del terminal o punto de terminación de red origen de la llamada, y de la del destino de la llamada. En caso de servicios móviles, se proporcionará una posición lo más exacta posible del punto de comunicación y, en todo caso, la identificación, localización y tipo de la estación base afectada.

8. Los sujetos obligados deberán facilitar al agente facultado, de entre los datos previstos en los apartados 5, 6 y 7 de este artículo, sólo aquéllos que estén incluidos en la orden de interceptación legal.

9. Con carácter previo a la ejecución de la orden de interceptación legal, los sujetos obligados deberán facilitar al agente facultado información sobre los servicios y características del sistema de telecomunicación que utilizan los sujetos objeto de la medida de la interceptación y, si obran en su poder, los correspondientes nombres de los abonados con sus números de documento nacional de identidad, tarjeta de identidad de extranjero o pasaporte, en el caso de personas físicas, o denominación y número de identificación fiscal en el caso de personas jurídicas.

10. Los sujetos obligados deberán tener en todo momento preparadas una o más interfaces a través de las cuales las comunicaciones electrónicas interceptadas y la información relativa a la interceptación se transmitirán a los centros de recepción de las interceptaciones. Las características de estas interfaces y el formato para la transmisión de las comunicaciones interceptadas a estos centros estarán sujetas a las especificaciones técnicas que se establezcan por el Ministerio de Asuntos Económicos y Transformación Digital.

11. En el caso de que los sujetos obligados apliquen a las comunicaciones objeto de interceptación legal algún procedimiento de compresión, cifrado, digitalización o cualquier otro tipo de codificación, deberán entregar aquellas desprovistas de los efectos de tales procedimientos, siempre que sean reversibles.

Las comunicaciones interceptadas deben proveerse al centro de recepción de las interceptaciones con una calidad no inferior a la que obtiene el destinatario de la comunicación.

Artículo 59. *Interceptación de las comunicaciones electrónicas por los servicios técnicos.*

1. Con pleno respeto al derecho al secreto de las comunicaciones y a la exigencia, conforme a lo establecido en la Ley de Enjuiciamiento Criminal, de autorización judicial para la interceptación de contenidos, cuando para la realización de las tareas de control para la eficaz utilización del dominio público radioeléctrico o para la localización de interferencias perjudiciales sea necesaria la utilización de equipos, infraestructuras e instalaciones técnicas de interceptación de señales no dirigidas al público en general, será de aplicación lo siguiente:

a) la administración de las telecomunicaciones deberá diseñar y establecer sus sistemas técnicos de interceptación de señales en forma tal que se reduzca al mínimo el riesgo de afectar a los contenidos de las comunicaciones;

b) cuando, como consecuencia de las interceptaciones técnicas efectuadas, quede constancia de los contenidos, los soportes en los que éstos aparezcan deberán ser custodiados hasta la finalización, en su caso, del expediente sancionador que hubiera lugar o, en otro caso, destruidos inmediatamente. En ninguna circunstancia podrán ser objeto de divulgación.

2. Las mismas reglas se aplicarán para la vigilancia del adecuado empleo de las redes y la correcta prestación de los servicios de comunicaciones electrónicas.

3. Lo establecido en este artículo se entiende sin perjuicio de las facultades que a la Administración atribuye el artículo 85.

Artículo 60. *Protección de los datos de carácter personal.*

1. Los operadores que suministren redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público, incluidas las redes públicas de comunicaciones que den soporte a dispositivos de identificación y recopilación de datos, deberán adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad en el suministro de su red o en la prestación de sus servicios, con el fin de garantizar la protección de los datos de carácter personal. Dichas medidas incluirán, como mínimo:

a) la garantía de que sólo el personal autorizado tenga acceso a los datos personales para fines autorizados por la ley;

b) la protección de los datos personales almacenados o transmitidos de la destrucción accidental o ilícita, la pérdida o alteración accidentales o el almacenamiento, tratamiento, acceso o revelación no autorizados o ilícitos;

c) la garantía de la aplicación efectiva de una política de seguridad con respecto al tratamiento de datos personales.

La Agencia Española de Protección de Datos, en el ejercicio de su competencia de garantía de la seguridad en el tratamiento de datos de carácter personal, podrá examinar las medidas adoptadas por los operadores que suministren redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público y podrá formular recomendaciones sobre las mejores prácticas con respecto al nivel de seguridad que debería conseguirse con estas medidas.

2. En caso de que exista un riesgo particular de violación de la seguridad de la red pública o del servicio de comunicaciones electrónicas, el operador que suministre dicha red o preste el servicio de comunicaciones electrónicas informará a los abonados sobre dicho riesgo y sobre las medidas a adoptar.

3. En caso de violación de los datos personales, el operador de servicios de comunicaciones electrónicas disponibles al público notificará sin dilaciones indebidas dicha violación a la Agencia Española de Protección de Datos. Si la violación de los datos pudiera afectar negativamente a la intimidad o a los datos personales de un abonado o particular, el operador notificará también la violación al abonado o particular sin dilaciones indebidas.

La notificación de una violación de los datos personales a un abonado o particular afectado no será necesaria si el operador ha probado a satisfacción de la Agencia Española de Protección de Datos que ha aplicado las medidas de protección tecnológica convenientes y que estas medidas se han aplicado a los datos afectados por la violación de seguridad. Unas medidas de protección de estas características podrían ser aquellas que convierten los datos en incomprensibles para toda persona que no esté autorizada a acceder a ellos.

Sin perjuicio de la obligación del operador de informar a los abonados o particulares afectados, si el operador no ha notificado ya al abonado o al particular la violación de los datos personales, la Agencia Española de Protección de Datos podrá exigirle que lo haga, una vez evaluados los posibles efectos adversos de la violación.

En la notificación al abonado o al particular se describirá al menos la naturaleza de la violación de los datos personales y los puntos de contacto donde puede obtenerse más información y se recomendarán medidas para atenuar los posibles efectos adversos de dicha violación. En la notificación a la Agencia Española de Protección de Datos se describirán además las consecuencias de la violación y las medidas propuestas o adoptadas por el operador respecto a la violación de los datos personales.

Los operadores deberán llevar un inventario de las violaciones de los datos personales, incluidos los hechos relacionados con tales infracciones, sus efectos y las medidas adoptadas al respecto, que resulte suficiente para permitir a la Agencia Española de Protección de Datos verificar el cumplimiento de las obligaciones de notificación reguladas en este apartado. Mediante real decreto podrá establecerse el formato y contenido del inventario.

A los efectos establecidos en este artículo, se entenderá como violación de los datos personales la violación de la seguridad que provoque la destrucción, accidental o ilícita, la pérdida, la alteración, la revelación o el acceso no autorizados, de datos personales

transmitidos, almacenados o tratados de otro modo en relación con la prestación de un servicio de comunicaciones electrónicas de acceso público.

La Agencia Española de Protección de Datos podrá adoptar directrices y, en caso necesario, dictar instrucciones sobre las circunstancias en que se requiere que el operador notifique la violación de los datos personales, sobre el formato que debe adoptar dicha notificación y sobre la manera de llevarla a cabo, con pleno respeto a las disposiciones que en su caso sean adoptadas en esta materia por la Comisión Europea.

4. Lo dispuesto en el presente artículo será sin perjuicio de la aplicación del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE y de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y su normativa de desarrollo.

Artículo 61. *Conservación y cesión de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.*

La conservación y cesión de los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación a los agentes facultados a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales se rige por lo establecido en la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

Artículo 62. *Cifrado en las redes y servicios de comunicaciones electrónicas.*

1. Cualquier tipo de información que se transmita por redes de comunicaciones electrónicas podrá ser protegida mediante procedimientos de cifrado.

2. El cifrado es un instrumento de seguridad de la información. Entre sus condiciones de uso, cuando se utilice para proteger la confidencialidad de la información, se podrá imponer la obligación de facilitar a un órgano de la Administración General del Estado o a un organismo público, los algoritmos o cualquier procedimiento de cifrado utilizado, en casos justificados de protección de los intereses esenciales de seguridad del Estado y la seguridad pública, y para permitir la investigación, la detección y el enjuiciamiento de delitos, así como la obligación de facilitar sin coste alguno los aparatos de cifra a efectos de su control de acuerdo con la normativa vigente.

3. Toda información obtenida por parte de la Administración General del Estado o cualquier organismo público a través de los preceptos incluidos en el apartado 2 de este artículo deberá ser tratada con la máxima confidencialidad y destruida una vez que se resuelva la amenaza para la seguridad del Estado y la seguridad pública o se haya dictado sentencia firme sobre el delito en cuestión.

Artículo 63. *Integridad y seguridad de las redes y de los servicios de comunicaciones electrónicas.*

1. Los operadores de redes públicas de comunicaciones electrónicas y de servicios de comunicaciones electrónicas disponibles al público, gestionarán adecuadamente los riesgos de seguridad que puedan afectar a sus redes y servicios a fin de garantizar un adecuado nivel de seguridad y evitar o reducir al mínimo el impacto de los incidentes de seguridad en los usuarios y en otras redes y servicios, para lo cual deberán adoptar las medidas técnicas y organizativas adecuadas, que deberán ser proporcionadas y en línea con el estado de la técnica, pudiendo incluir el cifrado.

2. Asimismo, los operadores de redes públicas de comunicaciones electrónicas garantizarán la integridad de las mismas a fin de asegurar la continuidad en la prestación de los servicios que utilizan dichas redes.

3. Los operadores que suministren redes públicas o presten servicios de comunicaciones electrónicas disponibles al público notificarán al Ministerio de Asuntos Económicos y

Transformación Digital los incidentes de seguridad que hayan tenido un impacto significativo en el suministro de las redes o los servicios.

Con el fin de determinar la importancia del impacto de un incidente de seguridad se tendrán en cuenta, en particular, los parámetros siguientes, cuando se disponga de ellos:

a) el número de usuarios afectados por el incidente de seguridad;
b) la duración del incidente de seguridad;
c) el área geográfica afectada por el incidente de seguridad;
d) la medida en que se ha visto afectado el funcionamiento de la red o del servicio;
e) el alcance del impacto sobre las actividades económicas y sociales.

Cuando proceda, el Ministerio informará a las autoridades nacionales competentes de otros Estados miembros y a la Agencia Europea de Seguridad en las Redes y la Información (ENISA). Asimismo, podrá informar al público o exigir a los operadores que lo hagan, en caso de estimar que la divulgación del incidente de seguridad reviste interés público. Una vez al año, el Ministerio presentará a la Comisión y a la ENISA un informe resumido sobre las notificaciones recibidas y las medidas adoptadas de conformidad con este apartado.

Del mismo modo, el Ministerio comunicará a la Secretaría de Estado de Seguridad del Ministerio del Interior aquellos incidentes que afectando a los operadores estratégicos nacionales sean de interés para la mejora de la protección de infraestructuras críticas, en el marco de la Ley 8/2011, de 28 de abril, reguladora de las mismas. También el Ministerio comunicará a la Comisión Nacional de los Mercados y la Competencia los incidentes de seguridad a que se refiere este apartado que afecten o puedan afectar a las obligaciones específicas impuestas por dicha Comisión en los mercados de referencia.

4. En caso de que exista una amenaza particular y significativa de incidente de seguridad en las redes públicas de comunicaciones electrónicas o en los servicios de comunicaciones electrónicas disponibles para el público, los operadores deberán informar a sus usuarios que pudieran verse afectados por dicha amenaza sobre las posibles medidas de protección o soluciones que pueden adoptar los usuarios. Cuando proceda, los operadores también informarán a sus usuarios sobre la propia amenaza.

5. El Ministerio de Asuntos Económicos y Transformación Digital establecerá los mecanismos para supervisar el cumplimiento de las obligaciones anteriores y, en su caso, dictará las instrucciones correspondientes, que serán vinculantes para los operadores, incluidas las relativas a las medidas necesarias adicionales a las identificadas por los operadores para solventar incidentes de seguridad, o impedir que ocurran cuando se haya observado una amenaza significativa, e incumplimientos de las fechas límite de aplicación. Entre las medidas relativas a la integridad y seguridad de redes y servicios de comunicaciones electrónicas que se puedan exigir a los operadores, podrá imponer:

a) la obligación de facilitar la información necesaria para evaluar la seguridad y la integridad de sus servicios y redes, incluidos los documentos sobre las políticas de seguridad;

b) la obligación de someterse a una auditoría de seguridad realizada por un organismo independiente o por una autoridad competente, y de poner el resultado a disposición del Ministerio de Asuntos Económicos y Transformación Digital. El coste de la auditoría será sufragado por el operador.

6. En particular, los operadores garantizarán la mayor disponibilidad posible de los servicios de comunicaciones vocales y de acceso a internet a través de las redes públicas de comunicaciones electrónicas en caso de fallo catastrófico de la red o en casos de fuerza mayor, y adoptarán todas las medidas necesarias para garantizar el acceso sin interrupciones a los servicios de emergencia y la transmisión ininterrumpida de las alertas públicas.

7. El presente artículo se entiende sin perjuicio de lo establecido en el artículo 4.6.

8. Lo dispuesto en el presente artículo será sin perjuicio de la aplicación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 y de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y su normativa de desarrollo.

CAPÍTULO IV

Derechos de los usuarios finales

Artículo 64. *Derechos de los usuarios finales y consumidores de servicios de comunicaciones electrónicas.*

1. Son titulares de los derechos específicos reconocidos en este capítulo, en las condiciones establecidas en el mismo, los usuarios finales y consumidores de servicios de comunicaciones electrónicas.

2. Los operadores que suministren redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público estarán obligados a respetar los derechos reconocidos en este capítulo. Las microempresas que presten servicios de comunicaciones interpersonales independientes de la numeración no estarán obligados a respetar los derechos reconocidos en este capítulo, salvo que también presten otros servicios de comunicaciones electrónicas. Estas microempresas deberán informar a los usuarios finales y consumidores antes de celebrar un contrato que se benefician de esta excepción y que, por tanto, no están obligadas a respetar los derechos reconocidos en este capítulo.

Tampoco están obligados a respetar los derechos reconocidos en este capítulo las empresas, autoridades públicas o usuarios finales que suministren el acceso a una red pública de comunicaciones electrónicas a través de RLAN, cuando dicho suministro no forme parte de una actividad económica o sea accesorio respecto de otra actividad económica o un servicio público que no dependa del transporte de señales por esas redes.

Las excepciones contempladas en el presente apartado lo serán sin perjuicio de la aplicación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 y de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y su normativa de desarrollo.

3. Las asociaciones de consumidores y usuarios y los operadores de comunicaciones electrónicas podrán negociar y aprobar códigos de conducta con el objetivo de mejorar la calidad general de la prestación de los servicios, que tendrán carácter vinculante exclusivamente entre los firmantes de los códigos.

4. El reconocimiento de los derechos específicos de los usuarios finales y consumidores de redes y servicios de comunicaciones electrónicas disponibles al público que efectúa este capítulo se entiende sin perjuicio de los derechos que otorga a los consumidores el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios aprobado por el Real Decreto Legislativo 1/2007, de 16 de noviembre, para aspectos no recogidos en la presente ley.

5. Las disposiciones que esta ley y su desarrollo reglamentario contienen en materia de derechos específicos de los usuarios finales y consumidores de servicios de comunicaciones electrónicas, en aquellos aspectos expresamente previstos en las disposiciones del derecho de la Unión Europea de las que traigan causa, serán de aplicación preferente en caso de conflicto con las disposiciones que regulen con carácter general los derechos de los consumidores y usuarios. La supervisión y control del correcto ejercicio de los derechos específicos de los usuarios finales y consumidores de servicios de comunicaciones electrónicas, así como la inspección y sanción por su incumplimiento, estará a cargo de la autoridad que se determine en esta ley y su desarrollo reglamentario.

Artículo 65. *Derechos específicos de los usuarios finales y consumidores de redes y servicios de comunicaciones electrónicas disponibles al público.*

1. Los derechos específicos de los usuarios finales y consumidores, según corresponda, de redes y servicios de comunicaciones electrónicas disponibles al público son, entre otros, los siguientes, que serán objeto de desarrollo mediante real decreto:

a) el derecho a celebrar contratos por parte de los usuarios finales con los operadores que presten servicios de comunicaciones electrónicas disponibles al público, así como el contenido mínimo de dichos contratos, en los términos establecidos en el artículo 67;

b) el derecho a rescindir el contrato anticipadamente y sin penalización en los supuestos contemplados en el artículo 67;

c) el derecho a la información, que deberá ser veraz, eficaz, suficiente, transparente, comparable, sobre los servicios de comunicaciones electrónicas disponibles al público, en virtud de lo dispuesto en el artículo 68;

d) el derecho a recibir información completa, comparable, pertinente, fiable, actualizada y de fácil consulta sobre la calidad de los servicios de comunicaciones electrónicas disponibles al público, en los términos establecidos en el artículo 69;

e) el derecho al cambio de operador, con conservación de los números del plan nacional de numeración en los supuestos y con los requisitos contemplados en el artículo 70;

f) el derecho a recibir información sobre las medidas adoptadas para garantizar un acceso equivalente para los usuarios finales con discapacidad, según lo dispuesto en el artículo 73;

g) el derecho a acceder a los servicios de emergencia a través de los servicios de comunicaciones de emergencia de forma gratuita sin tener que utilizar ningún medio de pago, según lo dispuesto en el artículo 74;

h) el derecho a acceder, a través de su servicio de acceso a internet, a la información y contenidos, así como a distribuirlos, usar y suministrar aplicaciones y servicios y utilizar los equipos terminales de su elección, con independencia de la ubicación del usuario final o del operador o de la ubicación, origen o destino de la información, contenido, aplicación o servicio, en los términos establecidos en el artículo 76;

i) el derecho a acceder a los servicios de comunicaciones electrónicas de voz, SMS y datos en itinerancia internacional, en particular, la itinerancia en la Unión Europea de conformidad con las condiciones, requisitos y tarifas reguladas en el Reglamento 531/2012 del Parlamento Europeo y del Consejo, de 13 de junio de 2012, relativo a la itinerancia en las redes públicas de comunicaciones móviles en la Unión;

j) el derecho a la facturación detallada, clara y sin errores, sin perjuicio del derecho a recibir facturas no desglosadas a petición del usuario.

Mediante real decreto se determinará el nivel básico de detalle en las facturas que los operadores habrán de ofrecer a los usuarios finales de manera gratuita, a fin de que estos puedan comprobar y controlar los gastos generados por el uso de los servicios de acceso a internet o servicios de comunicaciones vocales, o los servicios de comunicaciones interpersonales basados en numeración, así como efectuar un seguimiento adecuado de sus propios gastos y utilización, ejerciendo con ello un nivel razonable de control sobre sus facturas.

Dichas facturas detalladas incluirán una mención explícita de la identidad del operador;

k) el derecho de desconexión de determinados servicios.

Mediante real decreto de determinarán los supuestos, plazos y condiciones en que el usuario, previa solicitud, podrá ejercer el derecho de desconexión de determinados servicios y se contemplará la necesidad de petición expresa para el acceso a servicios de distinta consideración;

l) el derecho a acceder a servicios de tarificación adicional en las condiciones directamente asociadas al uso de la numeración para dichos servicios;

m) el derecho de los usuarios finales a solicitar al operador que ofrezca información sobre tarifas alternativas de menor precio, en caso de estar disponibles;

n) el derecho de los usuarios finales de desactivar la capacidad de terceros proveedores de servicios de aprovechar la factura de un operador de un servicio de acceso a internet o de un proveedor de un servicio de comunicaciones interpersonales disponible para el público, para cobrar por sus productos o servicios;

ñ) el derecho a detener el desvío automático de llamadas efectuado a su terminal por parte de un tercero;

o) el derecho a impedir, mediante un procedimiento sencillo y gratuito, la presentación de la identificación de su línea en las llamadas que genere o la presentación de la identificación de su línea al usuario que le realice una llamada.

Los usuarios finales no podrán ejercer este derecho cuando se trate de comunicaciones de emergencia a través del número de emergencia 112 o comunicaciones efectuadas a entidades que presten servicios de emergencia que se determinen mediante real decreto.

Por un período de tiempo limitado, los usuarios finales no podrán ejercer este derecho cuando el abonado a la línea de destino haya solicitado la identificación de las llamadas maliciosas o molestas realizadas a su línea;

p) el derecho a impedir, mediante un procedimiento sencillo y gratuito, la presentación de la identificación de la línea de origen en las llamadas entrantes y a rechazar las llamadas entrantes en que dicha línea no aparezca identificada.

En este supuesto y en el anterior, los operadores que presten servicios de comunicaciones interpersonales disponibles al público basados en la numeración, así como los que exploten redes públicas de comunicaciones electrónicas, deberán cumplir las condiciones que mediante real decreto se determinen sobre la visualización, restricción y supresión de la identificación de la línea de origen y conectada;

q) el derecho al reenvío de correos electrónicos o al acceso a los correos electrónicos una vez rescindido el contrato con un proveedor de servicios de acceso a internet.

Los usuarios finales que rescindan su contrato con un operador de servicios de acceso a internet, y que así lo soliciten, tienen el derecho bien a acceder a sus correos recibidos a las direcciones basadas en la denominación comercial o marca de su operador anterior o bien a que se le reenvíen los correos enviados a esa dirección a la nueva dirección que el usuario final indique. Tanto el acceso como el reenvío será gratuito para el usuario final;

r) el derecho a una especial protección en la utilización de servicios de tarificación adicional.

2. Los operadores deberán disponer de un servicio de atención al cliente, gratuito para los usuarios, que puede estar desvinculado de los servicios comerciales, que tenga por objeto facilitar información y atender y resolver las quejas y reclamaciones de sus clientes. Los servicios de atención al cliente mediante el canal telefónico deberán garantizar en todo momento una atención personal directa, más allá de la posibilidad de utilizar complementariamente otros medios técnicos a su alcance para mejorar dicha atención. Los operadores pondrán a disposición de sus clientes métodos para la acreditación documental de las gestiones o reclamaciones realizadas, como el otorgamiento de un número de referencia o la posibilidad de enviar al cliente un documento en soporte duradero.

3. En lo no previsto en esta ley, a los servicios de comunicaciones interpersonales disponibles al público independientes de la numeración les será de aplicación lo establecido en el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios, aprobado por el Real Decreto Legislativo 1/2007, de 16 de noviembre, en relación con los contratos de suministro de contenidos y servicios digitales.

4. Toda la información recibida por los usuarios finales y consumidores de redes y servicios de comunicaciones electrónicos disponibles al público, así como todos los servicios de atención al cliente deberán ser ofrecidos en la lengua oficial del Estado y en la lengua oficial de la Comunidad Autónoma correspondiente, cuando así sea requerido por el usuario final o consumidor.

Artículo 66. *Derecho a la protección de datos personales y la privacidad en relación con las comunicaciones no solicitadas, con los datos de tráfico y de localización y con las guías de abonados.*

1. Respecto a la protección de datos personales y la privacidad en relación con las comunicaciones no solicitadas los usuarios finales de los servicios de comunicaciones interpersonales disponibles al público basados en la numeración tendrán los siguientes derechos:

a) a no recibir llamadas automáticas sin intervención humana o mensajes de fax, con fines de comunicación comercial sin haber prestado su consentimiento previo para ello;

b) a no recibir llamadas no deseadas con fines de comunicación comercial, salvo que exista consentimiento previo del propio usuario para recibir este tipo de comunicaciones comerciales o salvo que la comunicación pueda ampararse en otra base de legitimación de las previstas en el artículo 6.1 del Reglamento (UE) 2016/679 de tratamiento de datos personales.

Véase, sobre la aplicación del apartado 1.b), la Circular de la Agencia Española de Protección de Datos de 26 de junio de 2023. Ref. BOE-A-2023-15071

2. Respecto a la protección de datos personales y la privacidad en relación con los datos de tráfico y los datos de localización distintos de los datos de tráfico, los usuarios finales de los servicios de comunicaciones interpersonales disponibles al público basados en la numeración tendrán los siguientes derechos:

a) a que se hagan anónimos o se cancelen sus datos de tráfico cuando ya no sean necesarios a los efectos de la transmisión de una comunicación. Los datos de tráfico necesarios a efectos de la facturación de los abonados y los pagos de las interconexiones podrán ser tratados únicamente hasta que haya expirado el plazo para la impugnación de la factura del servicio, para la devolución del cargo efectuado por el operador, para el pago de la factura o para que el operador pueda exigir su pago;

b) a que sus datos de tráfico sean utilizados para promoción comercial de servicios de comunicaciones electrónicas o para la prestación de servicios de valor añadido, en la medida y durante el tiempo necesarios para tales servicios o promoción comercial únicamente cuando hubieran prestado su consentimiento para ello. Los usuarios finales dispondrán del derecho de retirar su consentimiento para el tratamiento de los datos de tráfico en cualquier momento y con efecto inmediato;

c) a que sólo se proceda al tratamiento de sus datos de localización distintos a los datos de tráfico cuando se hayan hecho anónimos o previo su consentimiento y únicamente en la medida y por el tiempo necesarios para la prestación, en su caso, de servicios de valor añadido, con conocimiento inequívoco de los datos que vayan a ser sometidos a tratamiento, la finalidad y duración del mismo y el servicio de valor añadido que vaya a ser prestado. Los usuarios finales dispondrán del derecho de retirar su consentimiento en cualquier momento y con efecto inmediato para el tratamiento de los datos de localización distintos de tráfico.

Los usuarios finales no podrán ejercer este derecho cuando se trate de comunicaciones de emergencia a través del número de emergencia 112 o comunicaciones de emergencia efectuadas a entidades que presten servicios de emergencia que se determinen por el Ministerio de Asuntos Económicos y Transformación Digital.

3. Respecto a la protección de datos personales y la privacidad en relación con las guías de abonados y los servicios de información sobre números de abonado, los usuarios finales de los servicios de comunicaciones interpersonales disponibles al público basados en la numeración tendrán los siguientes derechos:

a) a figurar en las guías de abonados y a que sus datos sean usados para la prestación de los servicios de información sobre números de abonado;

b) a ser informados gratuitamente de la inclusión de sus datos en las guías y en los servicios de información sobre números de abonado, así como de la finalidad de las mismas, con carácter previo a dicha inclusión;

c) a no figurar en las guías o a solicitar la omisión de algunos de sus datos, en la medida en que tales datos sean pertinentes para la finalidad de la guía que haya estipulado su proveedor o para la finalidad de los servicios de información sobre números de abonados que se presenten en el mercado.

4. Lo establecido en las letras a) y c) del apartado 2 se entiende sin perjuicio de las obligaciones establecidas en la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

5. Lo dispuesto en este artículo será sin perjuicio de la aplicación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 y de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y su normativa de desarrollo, y, en particular, de la aplicación del concepto de consentimiento que figura en la misma.

Artículo 67. *Contratos.*

1. Antes de que un consumidor quede vinculado por un contrato o cualquier oferta correspondiente, los operadores que presten servicios de comunicaciones electrónicas disponibles al público distintos de los servicios de transmisión utilizados para la prestación de servicios máquina a máquina le facilitarán al menos la información que a estos efectos se establece en el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios aprobado por el Real Decreto Legislativo 1/2007, de 16 de noviembre.

Adicionalmente a lo establecido en el párrafo anterior, los operadores citados también proporcionarán, antes de la celebración del contrato, la información específica sobre el servicio de comunicaciones electrónicas de que se trate establecida en el anexo VIII del Código Europeo de Comunicaciones Electrónicas.

El operador facilitará dicha información de manera clara y comprensible en un soporte duradero, tal como se define en el artículo 59 bis.1.q) del texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios aprobado por el Real Decreto Legislativo 1/2007, de 16 de noviembre, o, en casos en los que un soporte duradero no sea viable, en un documento que se pueda descargar fácilmente. El operador llamará expresamente la atención del consumidor acerca de la disponibilidad de dicho documento y acerca de la importancia de su descarga con fines de documentación, referencia futura y reproducción sin cambios.

Esta información se proporcionará, previa petición, en un formato accesible para usuarios finales con discapacidad de acuerdo con la normativa por la que se armonizan los requisitos para productos y servicios.

2. Los operadores mencionados en el apartado anterior deben proporcionar a los consumidores un resumen del contrato conciso y de fácil lectura. Dicho resumen identificará los elementos principales del contrato referidos en el apartado anterior y, en todo caso, los siguientes:

a) el nombre, la dirección y la información de contacto del operador y, si fuera diferente, la información de contacto para las reclamaciones;

b) las características principales de cada servicio prestado;

c) los precios respectivos totales, incluyendo impuestos y tasas aplicables, por activar el servicio de comunicaciones electrónicas y por cualquier gasto recurrente o relacionado con el consumo, si el servicio se presta mediante un pago directo;

d) la duración del contrato y las condiciones para su renovación;

e) las condiciones y los mecanismos para solicitar la resolución del contrato, así como los costes asociados y posibles penalizaciones asociados a la rescisión del mismo;

f) en qué medida los productos y servicios están diseñados para usuarios finales con discapacidad;

g) con respecto a los servicios de acceso a internet, un resumen de la velocidad mínima, disponible normalmente, máxima y anunciada, descendente y ascendente de los servicios de acceso a internet en el caso de redes fijas, o de la velocidad máxima y anunciada estimadas descendente y ascendente de los servicios de acceso a internet en el caso de las redes móviles.

Los operadores deberán remitir, antes de la celebración del contrato, el contrato resumido de forma gratuita a los consumidores, incluso cuando se trate de contratos a distancia. Cuando por razones técnicas objetivas sea imposible facilitar el contrato resumido en el momento, se facilitará posteriormente sin demora indebida y el contrato será efectivo cuando el consumidor haya dado su consentimiento tras haber recibido el contrato resumido.

3. La información a que se refieren los dos apartados anteriores forma parte integrante del contrato y no se alterará a menos que las partes contratantes dispongan expresamente lo contrario.

4. Cuando los servicios de acceso a internet o los servicios de comunicaciones interpersonales disponibles al público se facturen en función del consumo de tiempo o de volumen, los operadores ofrecerán a los consumidores medios para vigilar y controlar el uso de cada uno de estos servicios. Estos medios incluirán el acceso a información oportuna sobre el nivel de consumo de los servicios incluidos en un plan de tarifas. En concreto, los operadores avisarán a los consumidores antes de alcanzar el límite de consumo

determinado mediante real decreto e incluido en su plan de tarifas y cuando se haya consumido completamente un servicio incluido en su plan de tarifas.

5. La información mencionada en los apartados anteriores se suministrará también a los usuarios finales que sean microempresas, pequeñas empresas y organizaciones sin ánimo de lucro, a menos que hayan acordado expresamente renunciar a la totalidad o parte de la información contenida en dichos apartados.

6. Mediante real decreto, previo informe de la Comisión Nacional de los Mercados y la Competencia, se podrá regular que los operadores deban facilitar más información sobre el nivel de consumo y, en su caso, impedir temporalmente la utilización del servicio correspondiente que supere un determinado límite financiero o de volumen.

7. Los contratos celebrados entre consumidores y operadores de servicios de comunicaciones electrónicas disponibles al público distintos de los servicios de transmisión utilizados para la prestación de servicios máquina a máquina, no tendrán un período de vigencia superior a veinticuatro meses. Esta duración también será aplicable a los contratos para dichos servicios suscritos con los usuarios finales que sean microempresas, pequeñas empresas u organizaciones sin ánimo de lucro, a menos que estas hayan acordado explícitamente renunciar a la misma.

El presente apartado no se aplicará a la duración de un contrato a plazos cuando el consumidor haya acordado en un contrato aparte efectuar pagos a plazos exclusivamente para el despliegue de una conexión física, en particular a redes de muy alta capacidad. Un contrato a plazos para el despliegue de una conexión física no incluirá terminales, como encaminadores o módems, y no impedirá a los consumidores ejercer sus derechos en virtud de lo dispuesto en el presente artículo.

Una vez que se cumpla el período de vigencia, dichos contratos quedan prorrogados automáticamente por el mismo periodo si bien, tras dicha prórroga, los usuarios finales tienen el derecho de rescindirlo en cualquier momento con un preaviso máximo de un mes sin contraer ningún coste excepto el de la recepción del servicio durante el período de preaviso. Con anterioridad a dicha prórroga automática, los operadores informarán a los usuarios finales de manera notoria y oportuna y en un soporte duradero de la finalización de los compromisos contractuales y los medios para rescindir el contrato y, de manera simultánea, el operador proporcionará a los usuarios finales información sobre las mejores tarifas de sus servicios. Los operadores facilitarán a los usuarios finales información sobre las mejores tarifas al menos una vez al año.

8. Los usuarios finales tienen el derecho de rescindir sus contratos sin contraer ningún coste adicional cuando el operador de los servicios de comunicaciones electrónicas disponibles al público les anuncie que propone introducir cambios en las condiciones contractuales, a menos que los cambios propuestos sean exclusivamente en beneficio del usuario final o sean de una naturaleza estrictamente administrativa y no tengan efectos negativos sobre los usuarios finales o vengan impuestos normativamente.

Los operadores comunicarán a los usuarios finales, al menos con un mes de antelación, cualquier cambio de las condiciones contractuales y les informarán al mismo tiempo de su derecho a rescindir su contrato sin contraer ningún coste adicional si no aceptan las nuevas condiciones. El derecho de rescindir el contrato podrá ejercerse en el plazo de un mes a partir de la comunicación, la cual debe efectuarse de forma clara y comprensible y en un soporte duradero.

En cualquier caso, únicamente podrán modificarse unilateralmente las condiciones de un contrato de servicios de comunicaciones electrónicas disponibles al público por los motivos válidos expresados en él.

9. Cualquier discrepancia significativa, ya sea continuada o frecuentemente recurrente, entre el rendimiento real de un servicio de comunicaciones electrónicas distinto del servicio de acceso a internet y distinto de un servicio de comunicaciones interpersonales independiente de la numeración, y el rendimiento indicado en el contrato se considerará un motivo para poder presentar las oportunas reclamaciones, en cuya resolución se podrá reconocer el derecho a rescindir el contrato sin coste alguno.

10. Cuando el usuario final tenga derecho a rescindir un contrato de servicio de comunicaciones electrónicas disponibles al público distinto de un servicio de comunicaciones interpersonales independiente de la numeración antes de que finalice el período fijado en el

contrato, el usuario final no deberá abonar ninguna compensación excepto por el equipo terminal subvencionado que conserve.

Cuando el usuario final decida conservar el equipo terminal incluido en el contrato en el momento de su finalización, la compensación debida no excederá de su valor prorrateado en el momento de la finalización del contrato o la parte restante de la tasa de servicio hasta el final del contrato, si esa cantidad fuera inferior.

Cualquier condición sobre el uso de los equipos terminales en otras redes será eliminada, de forma gratuita, por el operador a más tardar, tras el pago de dicha compensación.

11. En lo relativo a servicios de transmisión empleados para servicios máquina a máquina, los derechos a que se refieren los apartados 8 y 10 sólo deberán beneficiar a los usuarios finales que sean consumidores, microempresas o pequeñas empresas u organizaciones sin ánimo de lucro.

Artículo 68. *Transparencia, comparación de ofertas y publicación de información.*

1. Los operadores de servicios de acceso a internet o servicios de comunicaciones interpersonales disponibles al público deberán publicar la información relacionada con el contrato y los servicios que cubre con el fin de garantizar que todos los usuarios finales puedan elegir con conocimiento de causa. Esta información será, al menos, la establecida en el anexo IX del Código Europeo de Comunicaciones Electrónicas.

Esta información deberá ser proporcionada de manera clara, comprensible, en formato automatizado y fácilmente accesible para los usuarios finales con discapacidad, y deberá mantenerse actualizada regularmente.

2. El Ministerio de Asuntos Económicos y Transformación Digital, de acuerdo con las condiciones que se establezcan mediante real decreto, garantizará que los usuarios finales tengan acceso gratuito, al menos, a una herramienta de comparación independiente que les permita comparar y evaluar a los distintos servicios de acceso a internet y a los servicios de comunicaciones interpersonales disponibles al público basados en numeración y, cuando proceda, a los servicios de comunicaciones interpersonales disponibles al público independientes de la numeración, en lo que respecta a:

a) precios y tarifas de servicios proporcionados a cambio de pagos recurrentes o directos basados en el consumo;

b) la calidad de prestación del servicio cuando se ofrezca una calidad mínima de servicio o cuando el operador esté obligado a publicar esa información, de conformidad con lo dispuesto en el artículo 69.

3. Las herramientas de comparación deberán reunir los siguientes requisitos:

a) serán funcionalmente independientes de los proveedores de esos servicios, garantizando así que los proveedores de servicios reciben un trato equitativo en los resultados de las búsquedas;

b) indicarán claramente los propietarios y operadores de la herramienta de comparación;

c) establecerán criterios claros y objetivos en los que deberá basarse la comparación;

d) utilizarán un lenguaje sencillo e inequívoco;

e) proporcionarán información precisa y actualizada e indicarán el momento de la actualización más reciente;

f) estarán abiertas a cualquier proveedor de servicios de acceso a internet o de servicios de comunicaciones interpersonales disponibles al público de manera que pueda utilizar la información relevante e incluirán una amplia gama de ofertas que abarquen una parte significativa del mercado y, cuando la información presentada no proporcione una visión completa del mercado, una declaración clara a tal efecto antes de mostrar los resultados;

g) ofrecerán un procedimiento eficaz de notificación de errores en la información;

h) incluirán la posibilidad de comparar precios, tarifas y la calidad de prestación del servicio entre las ofertas disponibles para los consumidores, y entre dichas ofertas y las ofertas tipo disponibles para otros usuarios finales si así se requiriese.

Las herramientas de comparación, previa solicitud del proveedor de la herramienta, deberán ser certificadas por el Ministerio de Asuntos Económicos y Transformación Digital, en los términos en que se determine mediante real decreto.

La información publicada por los operadores de servicios de acceso a internet o de servicios de comunicaciones interpersonales disponibles al público podrá ser utilizada gratuitamente por terceros en formatos de datos abiertos, con el fin de hacer disponibles dichas herramientas de comparación independientes.

4. El Ministerio de Asuntos Económicos y Transformación Digital podrá exigir a los operadores que ofrezcan servicios de acceso a internet o servicios de comunicaciones interpersonales disponibles al público basados en numeración, o a ambos, que difundan de forma gratuita información de interés público a los antiguos y nuevos usuarios finales, cuando proceda, por las mismas vías que las utilizadas normalmente en sus comunicaciones con los usuarios finales. Dicha información, que será facilitada a los operadores en un formato normalizado, cubrirá, entre otros, los siguientes aspectos:

a) los usos más comunes de los servicios de acceso a internet y de los servicios de comunicaciones interpersonales disponibles al público basados en numeración para desarrollar actividades ilícitas o para difundir contenidos nocivos, en particular cuando ello puede atentar contra los derechos y libertades de terceros, incluyendo las infracciones de los derechos de protección de datos, los derechos de autor y derechos afines, así como sus consecuencias jurídicas;

b) los medios de protección contra los riesgos para la seguridad personal, la privacidad y los datos de carácter personal cuando utilicen los servicios de acceso a internet y los servicios de comunicaciones interpersonales disponibles al público basados en numeración.

5. El Ministerio de Asuntos Económicos y Transformación Digital publicará periódicamente los datos resultantes de la gestión del procedimiento de resolución de controversias establecido en el artículo 78.1. Los datos incluirán un nivel de desagregación que permita obtener información acerca de los servicios, materias y operadores sobre los que versan las reclamaciones recibidas.

6. Los operadores que presten a los consumidores servicios de comunicaciones electrónicas disponibles al público de acceso a internet o de comunicaciones interpersonales basados en el uso de la numeración, estarán obligados a comunicar al Ministerio de Asuntos Económicos y Transformación Digital, con al menos un mes de antelación a su entrada en vigor, todas las condiciones contractuales, tarifas y planes de precios conforme se establezca mediante real decreto, y entre ellos los siguientes:

a) las condiciones generales de contratación y cualquiera de sus modificaciones;

b) las tarifas y planes de precios que vayan a poner en el mercado, y cualquiera de sus modificaciones;

c) las condiciones particulares de todos los servicios, tarifas y planes de precios, así como sus modificaciones.

Artículo 69. *Calidad de servicio.*

1. La Comisión Nacional de los Mercados y la Competencia, previo informe de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, especificará los parámetros de calidad de servicio que habrán de cuantificarse y los métodos de medición aplicables, así como el contenido y formato de la información que deberá hacerse pública, incluidos posibles mecanismos de certificación de la calidad. Para ello, se tendrán en cuenta las directrices que establezca el ORECE y se utilizarán, si procede, los parámetros, definiciones y métodos de medición que figuran en el anexo X del Código Europeo de Comunicaciones Electrónicas.

2. La Comisión Nacional de los Mercados y la Competencia podrá exigir a los operadores de servicios de acceso a internet y de servicios de comunicaciones interpersonales disponibles al público la publicación de información completa, comparable, fiable, de fácil consulta y actualizada sobre la calidad de sus servicios destinada a los usuarios finales, en la medida en que controlan al menos algunos elementos de la red, ya sea directamente o en virtud de un acuerdo de nivel de servicio en este sentido, y sobre las

medidas adoptadas para garantizar un acceso equivalente para los usuarios finales con discapacidad.

La Comisión Nacional de los Mercados y la Competencia también podrá exigir a los operadores de servicios de comunicación interpersonal disponibles al público que informen a los consumidores, en caso de que la calidad de los servicios que suministran dependa de cualesquiera factores externos, como el control de la transmisión de la señal o la conectividad de red.

Previa petición, dicha información deberá ser facilitada, a la Comisión Nacional de los Mercados y la Competencia, con anterioridad a su publicación.

La Comisión Nacional de los Mercados y la Competencia realizará bienalmente un estudio de la calidad de servicio ofrecida a los usuarios finales radicados en las zonas rurales y escasamente pobladas respecto de la calidad media de servicio ofrecida al conjunto de usuarios radicados en el resto del país.

Las medidas que establezcan los operadores de servicios de acceso a internet y de servicios de comunicaciones interpersonales disponibles al público para garantizar la calidad de sus servicios, serán conformes al Reglamento (UE) 2015/2120, del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, por el que se establecen medidas en relación con el acceso a una internet abierta y tarifas al por menor para comunicaciones intracomunitarias reguladas y se modifican la Directiva 2002/22/CE y el Reglamento (UE) 531/2012.

Artículo 70. *Cambio de operador y conservación de los números por los usuarios finales.*

1. Los usuarios finales tienen derecho a cambiar de operador y los que tengan números del plan nacional de numeración tienen el derecho de conservar su número, previa solicitud, con independencia del operador que preste el servicio, al menos en los siguientes supuestos:

a) en una ubicación fija, cuando se trate de números geográficos;
b) en cualquier ubicación, si se trata de números no geográficos.

2. Cuando un usuario final rescinda un contrato con un operador, conservará el derecho a cambiar su número al nuevo operador durante, al menos, un mes después de la fecha de rescisión, a menos que el usuario final renuncie a ese derecho.

3. La conservación del número y su activación subsiguiente se ejecutarán con la mayor brevedad en la fecha o fechas acordadas explícitamente con el usuario final. En cualquier caso, a los usuarios finales que han suscrito un acuerdo para cambiar un número a un nuevo operador se les activará dicho número en el plazo de un día hábil desde la fecha acordada con el usuario final.

En caso de que el proceso de conservación del número falle, el operador donante reactivará el número o el servicio del usuario final hasta que dicho proceso finalice con éxito y continuará prestando sus servicios en las mismas condiciones hasta que se activen los servicios del operador receptor. En cualquier caso, la pérdida de servicio durante el proceso de cambio y conservación no excederá de un día hábil.

Los operadores cuyas redes de acceso o recursos sean utilizadas por el operador donante o por el receptor, o por ambos, velarán por que no haya pérdida de servicio que pueda retrasar los procesos de cambio o conservación.

4. En el caso de cambio de operador de servicios de acceso a internet, los operadores afectados facilitarán a los usuarios finales información adecuada antes y durante el proceso de transferencia y garantizarán la continuidad del servicio de acceso a internet, salvo que no sea posible técnicamente.

El operador receptor velará por que la activación del servicio de acceso a internet se produzca en el menor tiempo posible, en la fecha y en el horario expresamente acordados con el usuario final. El operador donante continuará prestando sus servicios de acceso a internet en las mismas condiciones hasta que el nuevo operador active a su vez los servicios de acceso a internet. La pérdida de servicio durante el proceso de transferencia no excederá de un día hábil.

5. El operador receptor dirigirá los procesos de cambio y conservación de números, debiendo cooperar de buena fe tanto el operador receptor como el operador donante. A tal efecto, ambos operadores no provocarán retrasos ni cometerán abusos relacionados con los

procesos de cambio y conservación ni cambiarán números. En particular, no se podrá transferir a los usuarios finales en contra de su voluntad o sin su consentimiento explícito.

El contrato del usuario final con el operador donante se rescindirá de forma automática con la finalización del proceso de cambio.

6. El proceso de cambio de operador y de conservación del número se regulará mediante real decreto, para lo cual deberá tenerse en cuenta la normativa en materia de consumidores y usuarios, la viabilidad técnica y la necesidad de mantener la continuidad del servicio al usuario final. En aplicación de este real decreto y su normativa de desarrollo, la Comisión Nacional de los Mercados y la Competencia podrá fijar, mediante circular, características y condiciones para el cambio de operador y la conservación de los números, así como los aspectos técnicos y administrativos necesarios para que ésta se lleve a cabo.

Esta regulación incluirá, cuando sea técnicamente viable, un requisito para que la conservación del número se complete mediante el aprovisionamiento inalámbrico de recursos, excepto cuando un usuario final solicite lo contrario.

La Comisión Nacional de los Mercados y la Competencia podrá adoptar medidas adecuadas que garanticen que los usuarios finales queden adecuadamente informados y protegidos durante todo el proceso de cambio y conservación.

7. Los operadores donantes reembolsarán, a petición del consumidor y sin dilaciones indebidas, cualquier crédito pendiente a los consumidores que usen servicios de prepago. El reembolso solo podrá estar sujeto a una tasa si se estipula así en el contrato. Esa tasa será proporcionada y adecuada a los costes reales asumidos por el operador donante al ofrecer el reembolso, a cuyos efectos la Comisión Nacional de los Mercados y la Competencia podrá requerir del operador donante cualquier información que permita acreditar este extremo.

8. El retraso y los abusos en materia de cambio de operador, de conservación de los números y en caso de no presentación a una cita de servicio y para la instalación, por parte de los operadores o en su nombre, dará derecho a los abonados a una compensación en los términos que se establezcan mediante real decreto, en el que se fijarán asimismo los supuestos en que dicha compensación será automática. Las condiciones y procedimientos para la resolución de los contratos no deberán constituir un factor disuasorio para cambiar de operador.

Artículo 71. *Contratos empaquetados.*

1. Si un contrato incluye un paquete de servicios o un paquete de servicios y equipos terminales ofrecidos a un consumidor, y al menos uno de estos servicios es un servicio de acceso a internet o servicios de comunicaciones interpersonales disponibles al público basados en numeración, se aplicarán a todos los elementos del paquete:

a) la obligación consistente en proporcionar al usuario final con carácter previo a la celebración del contrato un resumen del contrato conciso y de fácil lectura a que se refiere el artículo 67.2;

b) la obligación de proporcionar la información relacionada con el contrato y los servicios que cubre establecida en el artículo 67.1;

c) las condiciones sobre duración y resolución de los contratos establecidas en el artículo 67;

d) las condiciones para llevar a cabo el cambio de operador de servicios de acceso a internet establecidas en el artículo 70.4.

2. Cuando el consumidor tenga derecho a rescindir cualquier elemento del paquete de servicios o del paquete de servicios y equipos terminales contratado antes del vencimiento del plazo contractual, ya sea por razones de falta de adecuación con el contrato o ya sea por incumplimiento del suministro de los servicios, el consumidor tiene derecho a rescindir el contrato íntegro respecto a todos los elementos del paquete de servicios.

3. Cualquier abono a servicios adicionales prestados o a equipos terminales distribuidos por el mismo operador de los servicios de acceso a internet o de los servicios de comunicaciones interpersonales disponibles al público basados en numeración no prolongará el período original del contrato al que se han añadido dichos servicios o equipos terminales, a menos que el consumidor acepte expresamente lo contrario en el momento de contratar los servicios adicionales y los equipos terminales.

4. Los apartados 1 y 3 también se aplicarán a los usuarios finales que sean microempresas, pequeñas empresas u organizaciones sin ánimo de lucro, a menos que hayan acordado expresamente renunciar a la totalidad o parte de lo establecido en los mismos.

Artículo 72. *Guías de abonados y servicios de información sobre números de abonado.*

1. La elaboración y comercialización de las guías de abonados a los servicios de comunicaciones electrónicas y la prestación de los servicios de información sobre ellos se realizará en régimen de libre competencia.

2. Los operadores de servicios de comunicaciones interpersonales basados en numeración que asignan números de teléfono a partir de un plan de numeración habrán de dar curso a todas las solicitudes razonables de suministro de información pertinente para la prestación de los servicios de información sobre números de abonados y guías accesibles al público, en un formato acordado y en unas condiciones equitativas, objetivas, orientadas en función de los costes y no discriminatorias, estando sometidos el suministro de la citada información y su posterior utilización a la presente ley y su normativa de desarrollo.

La Comisión Nacional de los Mercados y la Competencia deberá suministrar gratuitamente los datos que le faciliten los citados operadores a las siguientes entidades:

a) entidades que elaboren guías telefónicas de abonados;

b) operadores que presten el servicio de consulta telefónica sobre números de abonado;

c) entidades que presten los servicios de llamadas de emergencia de conformidad con el artículo 74;

d) agentes facultados para realizar las interceptaciones que se autoricen de acuerdo con lo establecido en el artículo 58.2.

e) los servicios estadísticos oficiales para la elaboración de encuestas y el desarrollo de las competencias estadísticas que la ley les confiere, no siendo aplicable en este caso el derecho previsto en el artículo 66.3 c). La cesión se producirá de acuerdo con los principios recogidos en la normativa de protección de datos personales y con las siguientes garantías específicas:

1.º Se identificará en la solicitud el ámbito territorial respecto del cual se solicitan los números de teléfono.

2.º En el caso de encuestas de cumplimentación obligatoria, la solicitud y cesión de los números de teléfono deberán adecuarse a la metodología de la encuesta diseñada por el servicio estadístico oficial, de conformidad con las exigencias establecidas en la normativa reguladora de la función estadística pública.

3.º En el caso de encuestas y sondeos de cumplimentación voluntaria, la solicitud de números de teléfono no podrá referirse a un porcentaje de éstos superior al veinte por ciento de la población de dicho ámbito territorial, salvo que las características muestrales del estudio, o las dificultades para obtener una entrevista válida, exijan un porcentaje superior, debidamente justificado en la solicitud.

4.º En los supuestos de encuestas y sondeos de cumplimentación voluntaria, los números de teléfono sólo podrán ir segmentados y clasificados por las variables provincia, edad y sexo, tamaño de hábitat y situación laboral, debiendo ser en todo caso seleccionados de manera aleatoria de acuerdo con criterios estadísticos por parte de la Comisión Nacional de los Mercados y la Competencia de entre todos los disponibles en el ámbito solicitado, y debiendo ser números de teléfono anónimos no asociados al nombre del titular.

5.º Los números de teléfono cedidos son datos de contacto con los informantes y no podrán utilizarse para un fin distinto del identificado en la solicitud. Una solicitud podrá incluir, a efectos de sistematicidad, varios tratamientos independientes.

6.º Los números de teléfono cedidos de las unidades de la muestra deberán ser suprimidos una vez haya finalizado su colaboración en la operación estadística y los resultados hayan sido publicados. Los números de teléfono deberán estar disociados de las respuestas de los encuestados una vez finalizada la depuración de la información. En los supuestos de encuestas de cumplimentación voluntaria, en caso de no autorizarse la realización de la encuesta, el número de teléfono deberá ser inmediatamente suprimido.

7.º Cualquier dato que se publique a partir de las encuestas realizadas, deberá ser previamente anonimizado de acuerdo con la normativa de secreto estadístico.

El suministro de los datos por parte de la Comisión Nacional de los Mercados y la Competencia a las entidades previstas en las letras a), b), c) y d), se realizará de conformidad con las condiciones que se establezcan mediante real decreto y de acuerdo con el procedimiento para el suministro y recepción de la información que, en su caso, pueda fijar la Comisión Nacional de los Mercados y la Competencia mediante circular.

3. Se garantiza el acceso de los usuarios finales a los servicios de información sobre números de abonados, para cuya consecución la Comisión Nacional de los Mercados y la Competencia podrá imponer obligaciones y condiciones a las empresas que controlan el acceso a los usuarios finales en materia de prestación de servicios de información sobre números de abonado que deberán ser objetivas, equitativas, no discriminatorias y transparentes.

4. La Comisión Nacional de los Mercados y la Competencia adoptará medidas para garantizar el acceso directo de los usuarios finales al servicio de información sobre números de abonados de otro país comunitario mediante llamada vocal o SMS.

5. Lo dispuesto en el presente artículo se entenderá sin perjuicio de la aplicación de la normativa en materia de protección de datos personales aplicable.

Artículo 73. *Regulación de las condiciones básicas de acceso por personas con discapacidad.*

Mediante real decreto, oído en todo caso el Consejo Nacional de la Discapacidad, se podrán establecer las condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con las comunicaciones electrónicas. En la citada norma se establecerán los requisitos que deberán cumplir los operadores de servicios de comunicaciones electrónicas disponibles al público para garantizar que los usuarios con discapacidad:

a) puedan tener un acceso a servicios de comunicaciones electrónicas equivalente al que disfrutan la mayoría de los usuarios finales, incluida la información contractual, la facturación y la atención al público, en condiciones y formatos universalmente accesibles y con el uso de lenguas cooficiales;

b) se beneficien de la posibilidad de elección de operadores y servicios disponibles para la mayoría de usuarios finales.

Artículo 74. *Comunicaciones de emergencia y número de emergencia 112.*

1. Los usuarios finales de los servicios de comunicaciones interpersonales disponibles al público basados en numeración, cuando dichos servicios permitan realizar llamadas a un número de un plan de numeración nacional o internacional, incluidos los usuarios de los teléfonos públicos de pago, tienen derecho a acceder de manera gratuita, sin contraprestación económica de ningún tipo y sin tener que utilizar ningún medio de pago a los servicios de emergencia a través de comunicaciones de emergencia utilizando el número de emergencia 112 y otros números de emergencia que se determinen mediante real decreto.

En todo caso, el servicio de comunicaciones de emergencia será gratuito para los usuarios y para las autoridades receptoras de dichas comunicaciones de emergencia, cualquiera que sea la Administración Pública responsable de su prestación y con independencia del tipo de terminal que se utilice.

2. Los operadores de servicios de comunicaciones interpersonales disponibles al público basados en numeración, cuando dichos servicios permitan realizar llamadas a un número de un plan de numeración nacional o internacional, tienen la obligación de encaminar gratuitamente las comunicaciones de emergencia a los servicios de emergencia cuando se utilice el número de emergencia 112 u otros números de emergencia que se determinen.

Asimismo, los operadores citados pondrán a disposición de las autoridades receptoras de dichas comunicaciones de emergencia la información que mediante real decreto se determine relativa a la ubicación de las personas que efectúan la comunicación de emergencia, inmediatamente después del establecimiento de dicha comunicación. La

generación y transmisión de la información relativa a la localización del llamante es gratuita tanto para el llamante como para las autoridades receptoras de dichas comunicaciones de emergencia cuando se utilice el número de emergencia 112 u otros números de emergencia que se determinen.

Mediante real decreto se establecerán criterios para la precisión y la fiabilidad de la información facilitada sobre la ubicación de las personas que efectúan comunicaciones de emergencia a los servicios de emergencia.

La información relativa a la ubicación de las personas que efectúan la comunicación de emergencia únicamente podrá ser utilizada con la finalidad de facilitar la localización del llamante en relación con la concreta llamada de emergencia realizada.

3. El acceso a los servicios de emergencia a través de comunicaciones de emergencia para los usuarios finales con discapacidad será equivalente al que disfrutan otros usuarios finales. Mediante real decreto, oído en todo caso el Consejo Nacional de la Discapacidad, se establecerán las medidas adecuadas para garantizar que, en sus desplazamientos a otro Estado miembro de la Unión Europea, los usuarios finales con discapacidad puedan acceder a los servicios de emergencia en igualdad de condiciones que el resto de los usuarios finales y, si fuera factible, sin necesidad de registro previo. Estas medidas procurarán garantizar la interoperabilidad entre los Estados miembros y se basarán en la mayor medida posible en las normas o las especificaciones europeas pertinentes.

4. Las autoridades responsables de la prestación de los servicios de emergencia velarán por que los ciudadanos reciban una información adecuada sobre la existencia y utilización del número de emergencia 112, así como sus características de accesibilidad, y en particular, mediante iniciativas específicamente dirigidas a las personas que viajen a otros Estados miembros de la Unión Europea y a los usuarios finales con discapacidad.

5. Se promoverá el acceso a los servicios de emergencia a través del número de emergencia 112 y otros números de emergencia desde redes de comunicaciones electrónicas que no sean accesibles al público pero que permitan realizar llamadas a redes públicas, en concreto cuando la empresa responsable de dicha red no proporcione un acceso alternativo y sencillo a un servicio de emergencia.

6. Sin perjuicio de lo establecido en el presente artículo, a las comunicaciones de emergencia les será de aplicación el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y su normativa de desarrollo.

Artículo 75. *Sistemas de alertas públicas.*

1. Los operadores de servicios móviles de comunicaciones interpersonales basados en numeración deberán transmitir las alertas públicas en casos de grandes catástrofes o emergencias inminentes o en curso a los usuarios finales afectados, en los términos que se determinen mediante real decreto.

2. Adicionalmente a lo establecido en el apartado anterior, mediante real decreto se podrá establecer que las alertas públicas en casos de grandes catástrofes o emergencias inminentes o en curso se puedan transmitir por medio de otros servicios de comunicaciones electrónicas disponibles al público distintos de los indicados en el apartado anterior, por medio de servicios de comunicación audiovisual o por medio de una aplicación móvil basada en un servicio de acceso a través de internet, siempre que la eficacia del sistema de alerta sea equivalente en términos de cobertura y capacidad para abarcar a los usuarios finales, incluso aquellos que se encuentren de forma temporal en el área en cuestión.

3. Los usuarios finales deberán poder recibir las alertas fácilmente. La transmisión de alertas al público debe ser gratuita para los usuarios finales y para la entidad encargada de la emisión de las alertas.

Artículo 76. *Acceso abierto a internet.*

1. Los usuarios finales tienen el derecho a acceder, a través de su servicio de acceso a internet, a la información y contenidos, así como a distribuirlos, usar y suministrar aplicaciones y servicios y utilizar los equipos terminales de su elección, con independencia de la ubicación del usuario final o del operador o de la ubicación, origen o destino de la

información, contenido, aplicación o servicio, sin perjuicio de la normativa aplicable relativa a la licitud de los contenidos, aplicaciones y servicios.

2. Los acuerdos entre los operadores de servicios de acceso a internet y los usuarios finales sobre condiciones comerciales y técnicas y características de los servicios de acceso a internet como el precio, los volúmenes de datos o la velocidad, así como cualquier práctica comercial puesta en marcha por los operadores de servicios de acceso a internet, no limitarán el ejercicio de los derechos de los usuarios finales establecidos en el apartado anterior.

3. Los operadores de servicios de acceso a internet tratarán todo el tráfico de manera equitativa cuando presten servicios de acceso a internet, sin discriminación, restricción o interferencia, e independientemente del emisor y el receptor, el contenido al que se accede o que se distribuye, las aplicaciones o servicios utilizados o prestados, o el equipo terminal empleado.

Ello no impedirá que los operadores de servicios de acceso a internet apliquen medidas razonables de gestión del tráfico. Para ser consideradas razonables, dichas medidas deberán ser transparentes, no discriminatorias y proporcionadas, y no podrán basarse en consideraciones comerciales, sino en requisitos objetivamente diferentes de calidad técnica del servicio para categorías específicas de tráfico. Dichas medidas no supervisarán el contenido específico y no se mantendrán por más tiempo del necesario.

Los operadores de servicios de acceso a internet no tomarán medidas de gestión del tráfico que vayan más allá de las recogidas en el párrafo anterior y, en particular, no bloquearán, ralentizarán, alterarán, restringirán, interferirán, degradarán ni discriminarán entre contenidos, aplicaciones o servicios concretos o categorías específicas, excepto en caso necesario y únicamente durante el tiempo necesario para:

a) cumplir la normativa europea y nacional a la que el operador de servicio de acceso a internet esté sujeto, o dar cumplimiento a las sentencias judiciales;

b) preservar la integridad y la seguridad de la red, los servicios prestados a través de ella y los equipos terminales de los usuarios finales;

c) evitar la inminente congestión de la red y mitigar los efectos de congestiones de la red excepcionales o temporales, siempre que categorías equivalentes de tráfico se traten de manera equitativa.

4. Sólo se podrán tratar los datos personales para ejecutar las medidas de gestión del tráfico para el cumplimiento de los objetivos contemplados en el apartado anterior de acuerdo con los principios de necesidad y proporcionalidad y de conformidad con la presente ley y su normativa de desarrollo y con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y su normativa de desarrollo.

5. Los operadores de comunicaciones electrónicas disponibles al público, incluidos los operadores de servicios de acceso a internet y los proveedores de contenidos, aplicaciones y servicios, tendrán libertad para ofrecer servicios distintos a los servicios de acceso a internet que estén optimizados para contenidos, aplicaciones o servicios específicos o para combinaciones de estos, cuando la optimización sea necesaria para atender a las necesidades de contenidos, aplicaciones o servicios que precisen de un nivel de calidad específico.

Los operadores de comunicaciones electrónicas disponibles al público, incluidos los operadores de servicios de acceso a internet, podrán ofrecer o facilitar tales servicios únicamente si la capacidad de la red es suficiente para ofrecerlos además de los servicios de acceso a internet que ya se están prestando. Dichos servicios no serán utilizables u ofrecidos como sustitución de los servicios de acceso a internet y no irán en detrimento de la disponibilidad o de la calidad general de los servicios de acceso a internet para los usuarios finales.

6. Los operadores de servicios de acceso a internet se asegurarán de que cualquier contrato que incluya un servicio de acceso a internet especifique al menos la información siguiente:

a) información sobre cómo podrían afectar las medidas de gestión del tráfico aplicadas por el operador en cuestión a la calidad del servicio de acceso a internet, la intimidad de los usuarios fínales y la protección de sus datos personales;

b) una explicación clara y comprensible de la forma en que cualquier limitación del volumen de datos, la velocidad y otros parámetros de calidad del servicio pueden afectar en la práctica a los servicios de acceso a internet, especialmente a la utilización de contenidos, aplicaciones y servicios;

c) una explicación clara y comprensible de la manera en que cualquier servicio de los indicados en el apartado anterior, al que se suscriba el usuario final podrá afectar en la práctica a los servicios de acceso a internet proporcionados a dicho usuario final;

d) una explicación clara y comprensible de la velocidad mínima, disponible normalmente, máxima y anunciada, descendente y ascendente de los servicios de acceso a internet en el caso de redes fijas, o de la velocidad máxima y anunciada estimadas descendente y ascendente de los servicios de acceso a internet en el caso de las redes móviles, y la manera en que desviaciones significativas de las velocidades respectivas descendente y ascendente anunciadas podrían afectar al ejercicio de los derechos de los usuarios finales establecidos en el apartado 1;

e) una explicación clara y comprensible de las vías de resolución de reclamaciones y controversias disponibles para el consumidor en caso de surgir cualquier discrepancia, continua o periódicamente recurrente, entre el rendimiento real del servicio de acceso a internet en lo que respecta a la velocidad u otros parámetros de calidad del servicio y el rendimiento indicado de conformidad con las letras a) a d).

Los operadores de servicios de internet deberán publicar toda esta información.

7. Los operadores de servicios de acceso a internet implantarán procedimientos transparentes, sencillos y eficaces para hacer frente a las reclamaciones de los usuarios finales relacionadas con los derechos y obligaciones establecidos en este artículo.

8. Cualquier discrepancia significativa, ya sea continuada o periódicamente recurrente, entre el rendimiento real del servicio de acceso a internet en lo que se refiere a la velocidad u otros parámetros de calidad del servicio y el rendimiento indicado al público por el operador de servicios de acceso a internet de conformidad con el apartado 6, letras a) a d), se considerará, cuando los hechos pertinentes se establezcan mediante un mecanismo de supervisión certificado por una autoridad competente, como una falta de conformidad del rendimiento a efectos de abrir las vías de recurso disponibles para los consumidores.

9. El Ministerio de Asuntos Económicos y Transformación Digital supervisará la aplicación de lo establecido en este artículo y publicará un informe anual sobre dicha supervisión y sus resultados y lo remitirá a la Comisión Nacional de los Mercados y la Competencia, a la Comisión Europea y al ORECE.

Para llevar a cabo dicha supervisión, el Ministerio de Asuntos Económicos y Transformación Digital podrá solicitar a los operadores de servicios de comunicaciones electrónicas disponibles al público, incluidos los operadores de servicios de acceso a internet, con el grado de detalle oportuno, información pertinente a efecto de verificar el cumplimiento de las obligaciones establecidas en este artículo y, en particular, información sobre la gestión del tráfico en su red y su capacidad, así como podrá solicitar la aportación de los documentos que justifiquen todas las medidas de gestión del tráfico aplicadas.

Artículo 77. *Itinerancia en la Unión Europea y comunicaciones intracomunitarias reguladas.*

1. La regulación de la prestación de los servicios de comunicaciones electrónicas de voz, SMS y datos en itinerancia en la Unión Europea será la establecida en el Reglamento (UE) 531/2012 del Parlamento Europeo y del Consejo, de 13 de junio de 2012, relativo a la itinerancia en las redes públicas de comunicaciones móviles en la Unión y los reglamentos de ejecución que lo desarrollan.

2. La regulación de las tarifas al por menor de las comunicaciones interpersonales basadas en numeración intracomunitarias será la establecida en el Reglamento (UE) 2015/2120 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015.

Artículo 78. *Resolución de controversias.*

1. Los usuarios finales que sean personas físicas, incluidos los autónomos o trabajadores por cuenta propia, y las microempresas tendrán derecho a disponer de un procedimiento extrajudicial, transparente, no discriminatorio, sencillo y gratuito para resolver sus controversias con los operadores que suministren redes o presten servicios de comunicaciones electrónicas disponibles al público y otros agentes que intervienen el mercado de las telecomunicaciones, como los prestadores de servicios de tarificación adicional, cuando tales controversias se refieran a sus derechos específicos como usuarios finales de servicios de comunicaciones electrónicas reconocidos en esta ley y su normativa de desarrollo y de acuerdo con lo recogido en la normativa europea.

A tal fin, el Ministerio de Asuntos Económicos y Transformación Digital establecerá mediante orden un procedimiento conforme al cual, los usuarios finales podrán someterle dichas controversias, con arreglo a los principios establecidos en el apartado anterior. Los operadores y otros agentes que intervienen el mercado de las telecomunicaciones estarán obligados a someterse al procedimiento, así como a cumplir la resolución que le ponga fin. En cualquier caso, el procedimiento que se adopte establecerá el plazo máximo en el que deberá notificarse la resolución expresa, transcurrido el cual se podrá entender desestimada la reclamación por silencio administrativo, sin perjuicio de que el Ministerio de Asuntos Económicos y Transformación Digital tenga la obligación de resolver la reclamación de forma expresa, de acuerdo con lo establecido en el artículo 21 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. La resolución que se dicte podrá impugnarse ante la jurisdicción contencioso-administrativa.

Mediante real decreto se podrá prever que los usuarios finales que sean pequeñas y medianas empresas y organizaciones sin ánimo de lucro puedan también acceder a este procedimiento de resolución de controversias en defensa de sus derechos específicos de comunicaciones electrónicas.

2. Lo establecido en el apartado anterior se entiende sin perjuicio del derecho de los usuarios finales a someter las controversias al conocimiento de las Juntas arbitrales de consumo, de acuerdo con la legislación vigente en la materia. Si las Juntas arbitrales de consumo hubieran acordado el inicio de un procedimiento, no será posible acudir al procedimiento del apartado anterior a no ser que la solicitud haya sido archivada sin entrar en el fondo del asunto o las partes hayan desistido del procedimiento arbitral.

TÍTULO IV

Equipos de telecomunicación

Artículo 79. *Normalización técnica.*

1. Mediante real decreto se podrán establecer los supuestos y condiciones en que los operadores de redes públicas y servicios de comunicaciones electrónicas disponibles al público habrán de publicar las especificaciones técnicas precisas y adecuadas de las interfaces ofrecidas en España, con anterioridad a la posibilidad de acceso público a los servicios prestados a través de dichas interfaces.

2. Mediante real decreto se determinarán las formas de elaboración, en su caso, de las especificaciones técnicas aplicables a los equipos de telecomunicación, a efectos de garantizar el cumplimiento de los requisitos esenciales en los procedimientos de evaluación de conformidad y se fijarán los equipos exceptuados de la aplicación de dicha evaluación.

En los supuestos en que la normativa lo prevea, el Ministerio de Asuntos Económicos y Transformación Digital podrá aprobar especificaciones técnicas distintas de las anteriores para equipos de telecomunicación.

Artículo 80. *Requisitos esenciales y evaluación de conformidad de equipos de telecomunicación.*

1. Mediante real decreto se establecerán los requisitos esenciales que han de cumplir los equipos de telecomunicación y los procedimientos para la evaluación de su conformidad con dichos requisitos.

2. Los equipos de telecomunicación deberán evaluar su conformidad con los requisitos esenciales, ser conformes con todas las disposiciones que se establezcan e incorporar el marcado correspondiente como consecuencia de la evaluación realizada. Podrá exceptuarse de la aplicación de lo dispuesto en este título el uso de los equipos que mediante real decreto se determine, como los equipos de radioaficionados construidos por el propio usuario y no disponibles para venta en el mercado, conforme a lo dispuesto en su regulación específica.

3. El cumplimiento de todos los requisitos esenciales incluye la habilitación para la conexión de los equipos de telecomunicación destinados a conectarse a los puntos de terminación de una red pública de comunicaciones electrónicas. Dicho cumplimiento no supone autorización de uso para los equipos radioeléctricos sujetos a la obtención de autorización o concesión de dominio público radioeléctrico en los términos establecidos en esta ley.

4. Mediante real decreto se establecerán los requisitos que deben cumplir los organismos de evaluación de la conformidad, sus subcontratas y filiales y los procedimientos para su acreditación y para la evaluación y notificación a la Comisión Europea por el Ministerio de Asuntos Económicos y Transformación Digital, como Autoridad Notificante, de organismos de evaluación de la conformidad.

5. El Ministerio de Asuntos Económicos y Transformación Digital podrá promover procedimientos complementarios de certificación voluntaria para los equipos de telecomunicación que incluirán, al menos, la evaluación de la conformidad indicada en los apartados anteriores.

Artículo 81. *Reconocimiento mutuo.*

1. Los equipos de telecomunicación que hayan evaluado su conformidad con los requisitos esenciales en otro Estado miembro de la Unión Europea o en virtud de los acuerdos de reconocimiento mutuo celebrados por ella con terceros países, y cumplan con las demás disposiciones aplicables en la materia, tendrán la misma consideración, en lo que se refiere a lo dispuesto en este título, que los equipos cuya conformidad se ha verificado en España y cumplan, asimismo, las demás disposiciones legales en la materia.

2. El Ministerio de Asuntos Económicos y Transformación Digital establecerá los procedimientos para el reconocimiento de la conformidad de los equipos de telecomunicación a los que se refieren los acuerdos de reconocimiento mutuo que establezca la Unión Europea con terceros países.

3. Los equipos de telecomunicación que utilicen el espectro radioeléctrico con parámetros de radio no armonizados en la Unión Europea no podrán ser puestos en el mercado mientras no hayan sido autorizados por el Ministerio de Asuntos Económicos y Transformación Digital, además de haber evaluado la conformidad con las normas aplicables a aquéllos y ser conformes con el resto de disposiciones que les sean aplicables.

Artículo 82. *Importación, comercialización, puesta en servicio y uso de equipos de telecomunicación.*

1. Mediante real decreto se establecerán los requisitos para la importación, comercialización, puesta en servicio y uso de equipos de telecomunicación y las obligaciones aplicables a los distintos operadores económicos.

2. Para la importación de equipos de telecomunicación desde terceros países no pertenecientes a la Unión Europea, y para la comercialización, puesta en servicio y uso de estos equipos será requisito imprescindible que el operador económico establecido en la Unión Europea o el usuario final haya verificado previamente la conformidad de los equipos con los requisitos esenciales que les sean aplicables, así como el cumplimiento de las restantes disposiciones de aplicación.

3. Los equipos o sistemas sujetos a la obtención de concesiones, permisos o licencias solo podrán ser puestos en servicio y ser utilizados por los usuarios, en general, cuando hayan obtenido las citadas habilitaciones. Además, en el caso de equipos radioeléctricos, a fin de garantizar el uso eficaz y eficiente del espectro radioeléctrico, evitar interferencias perjudiciales o perturbaciones electromagnéticas, solo se permitirá la puesta en servicio de aquellos equipos que hayan sido fabricados de acuerdo con el uso del dominio público

radioeléctrico establecido en el Cuadro Nacional de Atribución de Frecuencias y de acuerdo con las interfaces de radio españolas, donde se define en cada caso, el uso del servicio, las frecuencias que pueden ser usadas y la potencia de las emisiones, así como otros parámetros radioeléctricos establecidos para la administración del dominio público radioeléctrico en España.

4. No está permitida la importación, comercialización, publicidad, cesión de forma gratuita u onerosa, instalación, tenencia, puesta en servicio o uso de cualquier equipo con funcionalidades para la generación intencionada de interferencias a equipos, redes o servicios de telecomunicaciones.

No obstante, se podrán llevar a cabo las actividades anteriores excepcionalmente por necesidades relacionadas con la seguridad pública, la defensa nacional, la seguridad nacional, la seguridad de la navegación aérea, la seguridad de la navegación marítima y la seguridad de las instituciones penitenciarias. Mediante real decreto se determinarán los mecanismos para su autorización y control.

Artículo 83. *Vigilancia del mercado de equipos de telecomunicación.*

1. La Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, como órgano administrativo encargado de la vigilancia del mercado de equipos de telecomunicación, garantizará que los equipos comercializados cumplan lo dispuesto en la normativa que resulte de aplicación, obligando a que se adapte el equipo a la normativa aplicable, se retire del mercado o se prohíba o restrinja su comercialización cuando no cumplan lo establecido en dicha normativa, no se utilice conforme al fin previsto o en las condiciones que razonablemente cabría prever, cuando su instalación o su mantenimiento no sean los adecuados, o cuando pueda comprometer la salud o seguridad de los usuarios.

2. Mediante real decreto se desarrollará el procedimiento para la vigilancia del mercado de equipos de telecomunicación, atribuyendo a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales la realización de los controles adecuados para asegurar que los equipos puestos en el mercado cumplen los requisitos aplicables.

3. La Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales podrá requerir a los operadores económicos implicados en la comercialización de los equipos las siguientes actuaciones:

a) la provisión de manera gratuita de los equipos comercializados para poder llevar a cabo los controles correspondientes;

b) la puesta a disposición de los documentos, las especificaciones técnicas, los datos o la información pertinentes en relación con la conformidad y los aspectos técnicos del producto, lo que incluye el acceso al software incorporado, en la medida en que dicho acceso sea necesario para evaluar la conformidad del producto con la normativa aplicable. La puesta a disposición será con independencia de la forma o formato y del soporte de almacenamiento o del lugar en que dichos documentos, especificaciones técnicas, datos o información estén almacenados. La puesta a disposición incluye la posibilidad de hacer u obtener copias de los documentos, especificaciones técnicas, datos o información;

c) la provisión de la información pertinente sobre la cadena de suministro, los detalles de la red de distribución, las cantidades de equipos en el mercado y otros modelos de equipos que tengan las mismas características técnicas que el equipo en cuestión, cuando sea pertinente para el cumplimiento de la normativa aplicable;

d) la provisión de la información pertinente que se requiera con miras a determinar la titularidad de los sitios web, cuando la información en cuestión esté relacionada con el objeto de la investigación;

e) cuando no se disponga de otros medios efectivos para eliminar un riesgo grave:

1.º la supresión del contenido relativo a los productos relacionados de una interfaz en línea, o para exigir que se muestre explícitamente una advertencia a los usuarios finales cuando accedan a una interfaz en línea o

2.º cuando no se atienda a un requerimiento con arreglo al anterior inciso 1.º, se podrá exigir a los proveedores de servicios de la sociedad de la información que restrinjan el acceso a la interfaz en línea, incluso pidiendo a un tercero pertinente que aplique dichas medidas.

4. Si la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales comprueba que un equipo de telecomunicación, a pesar de cumplir con lo establecido en la normativa que resulte de aplicación, presenta un riesgo para la salud o la seguridad de las personas o para otros aspectos de la protección del interés público, se solicitará al operador económico pertinente que adopte todas las medidas adecuadas para garantizar que el equipo de telecomunicación no presente ese riesgo cuando se introduzca en el mercado, o bien, para retirarlo del mercado o recuperarlo en el plazo de tiempo razonable, proporcional a la naturaleza del riesgo, que se determine.

5. La Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales podrá reclamar al operador económico responsable de la comercialización de los equipos la totalidad de los costes de sus actividades con respecto a casos de incumplimiento de la normativa que resulte de aplicación. Dichos costes podrán incluir los costes de los ensayos, los costes de almacenamiento y los costes de actividades relacionadas con equipos considerados no conformes.

6. Asimismo, la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales podrá proceder a la recuperación de equipos de telecomunicación de los usuarios que los posean cuando se hubieran causado interferencias perjudiciales o cuando se considere, justificadamente, que dichos equipos pueden causar las citadas interferencias.

Artículo 84. *Condiciones que deben cumplir las instalaciones e instaladores.*

1. La instalación de los equipos de telecomunicación deberá ser realizada siguiendo las instrucciones proporcionadas por el operador económico, manteniendo, en cualquier caso, inalteradas las condiciones bajo las cuales se ha verificado su conformidad con los requisitos esenciales, en los términos establecidos en los artículos anteriores de este título.

2. La prestación a terceros de servicios de instalación o mantenimiento de equipos o sistemas de telecomunicación se realizará en régimen de libre competencia sin más limitaciones que las establecidas en esta ley y su normativa de desarrollo.

Podrán prestar a terceros servicios de instalación o mantenimiento de equipos o sistemas de telecomunicación las personas físicas o jurídicas nacionales de un Estado miembro de la Unión Europea o con otra nacionalidad, cuando, en el segundo caso, así esté previsto en los acuerdos internacionales que vinculen al Reino de España. Para el resto de personas físicas o jurídicas, el Gobierno podrá autorizar excepciones de carácter general o particular a la regla anterior.

Mediante real decreto se establecerán los requisitos exigibles para el ejercicio de la actividad consistente en la prestación a terceros de servicios de instalación o mantenimiento de equipos o sistemas de telecomunicación relativos a la capacidad técnica y a la cualificación profesional para el ejercicio de la actividad, medios técnicos y cobertura mínima del seguro, aval o de cualquier otra garantía financiera. Los requisitos de acceso a la actividad y su ejercicio serán proporcionados, no discriminatorios, transparentes y objetivos, y estarán clara y directamente vinculados al interés general concreto que los justifique. Estos requisitos también serán exigibles para poder instalar o mantener equipos o sistemas de telecomunicación que vayan a utilizarse para prestar servicios de comunicaciones electrónicas disponibles al público.

3. Los interesados en la prestación a terceros de servicios de instalación o mantenimiento de equipos o sistemas de telecomunicación o en la instalación o mantenimiento de equipos o sistemas de telecomunicación que vayan a utilizarse para prestar servicios de comunicaciones electrónicas disponibles al público deberán, con anterioridad al inicio de la actividad, presentar al Registro de empresas instaladoras de telecomunicación, por medios electrónicos o telemáticos, una declaración responsable sobre el cumplimiento de los requisitos exigibles para el ejercicio de la actividad.

La declaración responsable habilita para la prestación a terceros de servicios de instalación o mantenimiento de equipos o sistemas de telecomunicación o para la instalación o mantenimiento de equipos o sistemas de telecomunicación que vayan a utilizarse para prestar servicios de comunicaciones electrónicas disponibles al público en todo el territorio español y con una duración indefinida.

Cuando se constate el incumplimiento de alguno de los requisitos determinados reglamentariamente, se le dirigirá al interesado una notificación para que subsane dicho

incumplimiento en el plazo de quince días hábiles. Transcurrido dicho plazo sin que la subsanación se hubiera producido, se procederá a dictar resolución privando de eficacia a la declaración y se cancelará la inscripción registral.

Cualquier hecho que suponga modificación de alguno de los datos incluidos en la declaración originaria deberá ser comunicado por el interesado por medios electrónicos o telemáticos, en el plazo máximo de un mes a partir del momento en que se produzca, a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, que procederá a la inscripción de la modificación en el Registro de empresas instaladoras de telecomunicación.

Si como consecuencia de la prestación de servicios de instalación o mantenimiento de equipos o sistemas de telecomunicación se pusiera en peligro la seguridad de las personas o de las redes públicas de telecomunicaciones, la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales podrá dictar resolución motivada por la que, previa audiencia del interesado, se adopte de forma cautelar e inmediata y por el tiempo imprescindible para ello la suspensión del ejercicio de la actividad de instalación para el interesado, sin perjuicio de que se pueda incoar el oportuno expediente sancionador de conformidad con lo establecido en el título VIII.

Será libre la prestación a terceros temporal u ocasional en el territorio español de servicios de instalación o mantenimiento de equipos o sistemas de telecomunicación por personas físicas o jurídicas legalmente establecidas en otros Estados miembros de la Unión Europea para el ejercicio de la misma actividad, sin perjuicio del cumplimiento de las obligaciones en materia de reconocimiento de cualificaciones profesionales que sean de aplicación a los profesionales que se desplacen.

4. El Registro de empresas instaladoras de telecomunicación será de carácter público y su regulación se hará mediante real decreto. En él se inscribirán de oficio los datos que se determinen mediante real decreto relativos a las personas físicas o jurídicas que hayan declarado su intención de prestar a terceros servicios de instalación o mantenimiento de equipos o sistemas de telecomunicación o de instalar o mantener equipos o sistemas de telecomunicación que vayan a utilizarse para prestar servicios de comunicaciones electrónicas disponibles al público y sus modificaciones, a partir de la información contenida en las declaraciones. Los trámites relativos a la inscripción en el mismo no podrán suponer un retraso de la habilitación para ejercer la actividad.

TÍTULO V

Dominio público radioeléctrico

Artículo 85. *De la administración del dominio público radioeléctrico.*

1. El espectro radioeléctrico es un bien de dominio público, cuya titularidad y administración corresponden al Estado. Dicha administración se ejercerá de conformidad con lo dispuesto en este título y en los tratados y acuerdos internacionales en los que España sea parte, atendiendo a la normativa aplicable en la Unión Europea y a las resoluciones y recomendaciones de la Unión Internacional de Telecomunicaciones y de otros organismos internacionales.

2. La administración del dominio público radioeléctrico se llevará a cabo teniendo en cuenta su importante valor social, cultural y económico y la necesaria cooperación con otros Estados miembros de la Unión Europea y con la Comisión Europea en la planificación estratégica, la coordinación y la armonización del uso del espectro radioeléctrico en la Unión Europea.

En el marco de dicha cooperación se fomentará la coordinación de los enfoques políticos en materia de espectro radioeléctrico en la Unión Europea y, cuando proceda, la armonización de las condiciones necesarias para la creación y el funcionamiento del mercado interior de las comunicaciones electrónicas. Para ello, se tendrán en cuenta, entre otros, los aspectos económicos, de seguridad, de salud, de interés público, de libertad de expresión, de derechos de los consumidores, culturales, científicos, sociales y técnicos de las políticas de la Unión Europea, así como los diversos intereses de las comunidades de usuarios del espectro, atendiendo siempre a la necesidad de garantizar un uso eficiente y

efectivo de las radiofrecuencias y a los beneficios para los consumidores, como la realización de economías de escala y la interoperabilidad de los servicios y redes.

En esa labor, la administración del dominio público radioeléctrico perseguirá, entre otras finalidades:

a) procurar la cobertura de banda ancha inalámbrica del territorio y la población en condiciones de alta calidad y velocidad, así como la cobertura de los grandes corredores de transporte;

b) facilitar el rápido desarrollo de nuevas tecnologías y aplicaciones inalámbricas al servicio de las comunicaciones, incluido, cuando sea oportuno, el enfoque intersectorial;

c) garantizar la previsibilidad y coherencia en la concesión, renovación, modificación, restricción o supresión de los derechos de utilización del dominio público radioeléctrico con miras a promover inversiones a largo plazo;

d) procurar la prevención de las interferencias perjudiciales, y adoptar a tal fin medidas apropiadas, tanto preventivas como correctoras;

e) promover el uso compartido del espectro radioeléctrico entre usos similares o diferentes de conformidad con la normativa de competencia;

f) aplicar el sistema de autorización más apropiado y menos oneroso posible, de forma que se maximice la flexibilidad, el uso compartido y el uso eficiente en el uso del dominio público radioeléctrico;

g) aplicar normas para la concesión, cesión, renovación, modificación y supresión de derechos de uso del dominio público radioeléctrico que estén definidas de forma clara y transparente de forma que se asegure la certidumbre, coherencia y previsibilidad;

h) preservar la salud de la población mediante la determinación, control e inspección de los niveles únicos de emisión radioeléctrica tolerable que no supongan un peligro para la salud pública.

3. En particular, son principios aplicables a la administración del dominio público radioeléctrico, entre otros, los siguientes:

a) garantizar un uso eficaz y eficiente de este recurso;

b) fomentar la neutralidad tecnológica y de los servicios, y el mercado secundario del espectro;

c) fomentar una mayor competencia en el mercado de las comunicaciones electrónicas.

4. La administración del dominio público radioeléctrico tiene por objetivo el establecimiento de un marco jurídico que asegure unas condiciones armonizadas para su uso y que permita su disponibilidad y uso eficiente, y abarca un conjunto de actuaciones entre las cuales se incluyen las siguientes:

a) planificación: Elaboración y aprobación de los planes de utilización;

b) gestión: Establecimiento, de acuerdo con la planificación previa, de las condiciones técnicas de explotación y otorgamiento de los derechos de uso;

c) control: Comprobación técnica de las emisiones, detección y eliminación de interferencias, inspección técnica de instalaciones, equipos radioeléctricos, así como el control de la comercialización, la puesta en servicio y el uso de éstos últimos.

Igualmente, incluye la protección del dominio público radioeléctrico, consistente, entre otras actuaciones, en la realización de emisiones sin contenidos sustantivos en aquellas frecuencias y canales radioeléctricos cuyos derechos de uso, en el ámbito territorial correspondiente, no hayan sido otorgados, con independencia de que dichas frecuencias o canales radioeléctricos sean objeto en la práctica de ocupación o uso efectivo;

d) aplicación del régimen sancionador.

5. La utilización de frecuencias radioeléctricas mediante redes de satélites se incluye dentro de la administración del dominio público radioeléctrico.

Asimismo, la utilización del dominio público radioeléctrico necesaria para la utilización de los recursos órbita-espectro en el ámbito de la soberanía española y mediante satélites de comunicaciones queda reservada al Estado. Su explotación estará sometida al derecho internacional y se realizará, en la forma que mediante real decreto se determine, mediante su gestión directa por el Estado o mediante concesión, en el que se fijará asimismo su

duración. En todo caso, la gestión podrá también llevarse a cabo mediante conciertos con organismos internacionales.

Artículo 86. *Facultades del Gobierno para la administración del dominio público radioeléctrico.*

El Gobierno desarrollará mediante real decreto las condiciones para la adecuada administración del dominio público radioeléctrico. En dicho real decreto se regulará, como mínimo, lo siguiente:

a) el procedimiento para la elaboración de los planes de utilización del espectro radioeléctrico, que incluyen el Cuadro Nacional de Atribución de Frecuencias, los planes técnicos nacionales de radiodifusión y televisión, cuya aprobación corresponderá al Gobierno, y las necesidades de espectro radioeléctrico para la defensa nacional. Los datos relativos a esta última materia tendrán el carácter de reservados;

b) el procedimiento de determinación, control e inspección de los niveles únicos de emisión radioeléctrica tolerable y que no supongan un peligro para la salud pública, que deberán ser respetados en todo caso y momento por las diferentes instalaciones o infraestructuras a instalar y ya instaladas que hagan uso del dominio público radioeléctrico. En la determinación de estos niveles únicos de emisión radioeléctrica tolerable se tendrá en cuenta tanto criterios técnicos en el uso del dominio público radioeléctrico, como criterios de preservación de la salud de las personas y en concordancia con lo dispuesto por las recomendaciones de la Comisión Europea. Tales límites deberán ser respetados, en todo caso, por el resto de Administraciones públicas, tanto autonómicas como locales, que no podrán modificarlos ni de manera directa, en términos de densidad de potencia o de intensidad de campo eléctrico, ni de manera indirecta mediante el establecimiento de distancias mínimas de protección radioeléctrica;

c) los procedimientos, plazos y condiciones para la habilitación del ejercicio de los derechos de uso del dominio público radioeléctrico, que revestirá la forma de autorización general, autorización individual, afectación o concesión administrativas.

En particular, se regularán los procedimientos abiertos de otorgamiento de derechos de uso del dominio público radioeléctrico, que se basarán en criterios de elegibilidad fijados de antemano, objetivos, transparentes, no discriminatorios, proporcionados y que reflejen las condiciones asociadas a tales derechos.

No obstante lo anterior, cuando resulte necesario el otorgamiento de derechos individuales de utilización de radiofrecuencias a prestadores de servicios de comunicación audiovisual radiofónicos o televisivos para lograr un objetivo de interés general establecido de conformidad con el Derecho de la Unión Europea, podrán establecerse excepciones al requisito de procedimiento abierto;

d) el procedimiento para la reasignación del uso de bandas de frecuencias con el objetivo de alcanzar un uso más eficiente del espectro radioeléctrico, en función de su idoneidad para la prestación de nuevos servicios o de la evaluación de las tecnologías, que podrá incluir el calendario de actuaciones y la evaluación de los costes asociados, en particular, los ocasionados a los titulares de derechos de uso afectados por estas actuaciones de reasignación, que podrán verse compensados a través de un fondo económico o cualquier otro mecanismo de compensación que se establezca;

e) las condiciones no discriminatorias, proporcionadas y transparentes asociadas a los títulos habilitantes para el uso del dominio público radioeléctrico, entre las que se incluirán las necesarias para garantizar el uso efectivo y eficiente de las frecuencias y los compromisos contraídos por los operadores en los procesos de licitación previstos en el artículo 89. Estas condiciones buscarán promover en todo caso la consecución de los mayores beneficios posibles para los usuarios, así como mantener los incentivos suficientes para la inversión y la innovación;

f) las condiciones de otorgamiento de títulos habilitantes para el uso del dominio público radioeléctrico para fines experimentales o eventos de corta duración;

g) la adecuada utilización del espectro radioeléctrico mediante el empleo de equipos y aparatos.

Artículo 87. *Coordinación transfronteriza del espectro radioeléctrico.*

1. El Ministerio de Asuntos Económicos y Transformación Digital llevará a cabo una administración del espectro radioeléctrico de forma que no se impida a ningún otro Estado miembro de la Unión Europea permitir en su territorio el uso del espectro radioeléctrico armonizado de conformidad con la legislación de la Unión Europea, principalmente en lo relativo a evitar interferencias perjudiciales transfronterizas entre los Estados miembros, sin perjuicio del cumplimiento de la legislación internacional y de los acuerdos internacionales pertinentes, como el Reglamento de Radiocomunicaciones de la Unión Internacional de Telecomunicaciones (UIT) y los acuerdos regionales de radiocomunicaciones de la UIT.

2. Se cooperará con los Estados miembros de la Unión Europea y, cuando proceda, a través del Grupo de Política del Espectro Radioeléctrico (RSPG, en inglés), en la coordinación transfronteriza en el uso del espectro radioeléctrico al objeto de:

a) garantizar el uso del espectro radioeléctrico armonizado de conformidad con la legislación de la Unión Europea;

b) resolver cualquier problema o disputa en relación con la coordinación transfronteriza o con las interferencias perjudiciales transfronterizas entre Estados miembros o con terceros países que impiden hacer uso del espectro radioeléctrico armonizado.

3. En esta labor de coordinación transfronteriza del espectro radioeléctrico, el Ministerio de Asuntos Económicos y Transformación Digital podrá solicitar la colaboración y el apoyo del RSPG para hacer frente a cualquier problema o disputa en relación con la coordinación transfronteriza o con las interferencias perjudiciales transfronterizas. En su caso, el RSPG podrá emitir un dictamen en el que proponga una solución coordinada en relación con dicho problema o disputa.

4. El Ministerio de Asuntos Económicos y Transformación Digital podrá solicitar a las instituciones europeas apoyo jurídico, político y técnico a fin de resolver problemas de coordinación del espectro radioeléctrico con países vecinos de la Unión Europea.

5. El Ministerio de Asuntos Económicos y Transformación Digital cooperará con el fin de coordinar el uso del espectro radioeléctrico armonizado para redes y servicios de comunicaciones electrónicas en la Unión Europea. Ello puede incluir determinar una o, cuando sea pertinente, varias fechas límite comunes para la autorización de bandas específicas del espectro radioeléctrico armonizado.

6. El Ministerio de Asuntos Económicos y Transformación Digital cooperará con los órganos competentes de otros Estados fuera de la Unión Europea para resolver de forma temprana y eficaz cualquier problema o disputa en relación con terceros países que impiden hacer uso del espectro radioeléctrico, de forma que se garantice el cumplimiento de la legislación internacional y de los acuerdos internacionales pertinentes, como el Reglamento de Radiocomunicaciones de la Unión Internacional de Telecomunicaciones (UIT) y los acuerdos regionales de radiocomunicaciones de la UIT.

Artículo 88. *Títulos habilitantes para el uso del dominio público radioeléctrico.*

1. El uso del dominio público radioeléctrico podrá ser común, especial o privativo.

El uso común del dominio público radioeléctrico no precisará de ningún título habilitante y se llevará a cabo en las bandas de frecuencias y con las características técnicas que se establezcan al efecto. No obstante, los operadores que hagan uso de bandas de frecuencias de uso común deberán comunicar a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales los siguientes datos:

a) las bandas de frecuencias de funcionamiento de sus redes que hagan un uso común del dominio público radioeléctrico;

b) los datos descriptivos de la zona de servicio de cada una de las redes del operador que hagan un uso común del dominio público radioeléctrico, incluyendo el tipo de cobertura (municipal, provincial, autonómica o estatal), así como los identificadores de cada red;

c) el número de transmisores de cada red que hagan un uso común del dominio público radioeléctrico, así como los datos técnicos actualizados de los transmisores de cada red, incluyendo sus coordenadas geográficas.

El uso especial del dominio público radioeléctrico es el que se lleve a cabo de las bandas de frecuencias habilitadas para su explotación de forma compartida, sin limitación de número de operadores o usuarios y con las condiciones técnicas y para los servicios que se establezcan en cada caso.

El uso privativo del dominio público radioeléctrico es el que se realiza mediante la explotación en exclusiva o por un número limitado de usuarios de determinadas frecuencias en un mismo ámbito físico de aplicación.

2. Para el acceso a una red pública de comunicaciones electrónicas a través de RLAN, cuando dicho acceso no forme parte de una actividad económica o sea accesorio respecto de otra actividad económica o un servicio público que no dependa del transporte de señales por esas redes, las empresas, autoridades públicas o usuarios finales que suministren el acceso no estarán sujetos a la previa obtención de un título habilitante, sin perjuicio de que el uso del dominio público radioeléctrico deba llevarse a cabo en las bandas de frecuencias y con las características técnicas que se establezcan al efecto.

3. Los títulos habilitantes mediante los que se otorguen derechos de uso del dominio público radioeléctrico revestirán la forma de autorización general, autorización individual, afectación o concesión administrativas. El plazo para el otorgamiento de los títulos habilitantes será de seis semanas desde la entrada de la solicitud en cualquiera de los registros del órgano administrativo competente, sin perjuicio de lo establecido para los derechos de uso con limitación de número. Dicho plazo no será de aplicación cuando sea necesaria la coordinación internacional de frecuencias o afecte a reservas de posiciones orbitales.

4. El otorgamiento de derechos de uso del dominio público radioeléctrico revestirá la forma de autorización general en los supuestos de uso especial de las bandas de frecuencia habilitadas a tal efecto a través de redes públicas de comunicaciones electrónicas suministradas por operadores de comunicaciones electrónicas.

La autorización general se entenderá concedida sin más trámite que la notificación a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, mediante el procedimiento y con los requisitos que se establezcan mediante orden de la persona titular del Ministerio de Asuntos Económicos y Transformación Digital, sin perjuicio de la obligación de abono de las tasas correspondientes. Cuando dicha Secretaría de Estado constate que la notificación no reúne los requisitos establecidos anteriormente, dictará resolución motivada en un plazo máximo de quince días hábiles, no teniendo por realizada aquélla.

5. El otorgamiento de derechos de uso del dominio público radioeléctrico revestirá la forma de autorización individual en los siguientes supuestos:

a) si se trata de una reserva de derecho de uso especial por radioaficionados u otros sin contenido económico en cuya regulación específica así se establezca;

b) si se otorga el derecho de uso privativo para autoprestación por el solicitante, salvo en el caso de Administraciones públicas, que requerirán de afectación demanial.

6. En el resto de los supuestos no contemplados en los apartados anteriores, el derecho al uso privativo del dominio público radioeléctrico requerirá una concesión administrativa. Para el otorgamiento de dicha concesión, será requisito previo que los solicitantes ostenten la condición de operador de comunicaciones electrónicas y que en ellos no concurra alguna de las prohibiciones de contratar reguladas en la Ley de Contratos del Sector Público, aprobado por la Ley 9/2017, de 8 de noviembre.

Las concesiones de uso privativo del dominio público radioeléctrico reservado para la prestación de servicios de comunicación audiovisual se otorgarán por la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales aneja al título habilitante audiovisual, ya consista este título habilitante en una licencia o en la habilitación para la prestación de servicios públicos de comunicación audiovisual conforme a lo establecido en la normativa de servicios de comunicación audiovisual. La duración de estas concesiones será la del título habilitante audiovisual. En estos supuestos, el operador en cuyo favor se otorgue la concesión no tiene por qué ostentar la condición de operador de comunicaciones electrónicas sino la de prestador de servicios de comunicación audiovisual.

7. En caso de falta de demanda a nivel nacional o inferior de uso de una banda en el dominio público radioeléctrico sujeto a condiciones armonizadas, la Secretaría de Estado de

Telecomunicaciones e Infraestructuras Digitales podrá permitir un uso alternativo de dicha banda o de parte de ella, incluido el uso existente, a condición de que:

a) el descubrimiento de la falta de demanda de uso de tal banda se base en una consulta pública por un plazo no inferior a treinta días naturales, incluida una evaluación prospectiva de la demanda en el mercado;

b) el citado uso alternativo no impida o entorpezca la disponibilidad del uso de la banda armonizada en otros Estados miembros, y

c) tenga debidamente en cuenta la disponibilidad o el uso a largo plazo de la banda armonizada, así como las economías de escala para los equipos que resultan del uso del espectro radioeléctrico armonizado.

La decisión que permita el uso alternativo de forma excepcional de una banda o parte de ella estará sujeta a revisión periódica, y en cualquier caso se revisará con prontitud a raíz de una petición debidamente justificada de uso de la banda de conformidad con las condiciones armonizadas.

8. Es competencia de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales el otorgamiento de los títulos habilitantes, salvo en los supuestos de otorgamiento por procedimiento de licitación contemplado en el artículo 89.

Las resoluciones mediante las cuales se otorguen los títulos habilitantes de dominio público radioeléctrico se dictarán en la forma y plazos que se establezcan mediante real decreto que establecerá, asimismo, la información que se hará pública sobre dichas concesiones.

9. Los operadores que resultasen seleccionados para la asignación o reserva a su favor de derechos de uso del espectro radioeléctrico efectuada por las instituciones de la Unión Europea o derivada de acuerdos internacionales, se inscribirán de oficio en el Registro de operadores. La Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales otorgará la concesión demanial a los operadores antes mencionados. En las citadas concesiones se incluirán, entre otras, las condiciones que procedan establecidas en los procedimientos de asignación o reserva, así como los compromisos adquiridos por el operador en dichos procedimientos, sin que se puedan imponer condiciones o criterios adicionales ni procedimientos que limiten, alteren o demoren la correcta aplicación de la asignación común de dicho espectro radioeléctrico.

10. El Ministerio de Asuntos Económicos y Transformación Digital, teniendo en cuenta los intereses manifestados por los agentes intervinientes en el mercado de las telecomunicaciones y previo informe de la Comisión Nacional de los Mercados y la Competencia, podrá cooperar con las autoridades competentes de otros Estados miembros de la Unión Europea y con el Grupo de Política del Espectro Radioeléctrico (RSPG) para establecer conjuntamente los aspectos comunes de un proceso de asignación de derechos de uso del dominio público radioeléctrico y, en su caso, desarrollar también conjuntamente el proceso de selección para el otorgamiento de títulos habilitantes del uso del dominio público radioeléctrico.

Al concebir el proceso de asignación conjunta, se podrá tener en cuenta los siguientes criterios:

a) los distintos procesos de asignación nacionales serán iniciados y desarrollados por las autoridades competentes de conformidad con un calendario aprobado conjuntamente;

b) dispondrá, en su caso, unas condiciones y procedimientos comunes para la selección y otorgamiento de los títulos habilitantes de uso del dominio público radioeléctrico;

c) dispondrá, si procede, unas condiciones comunes o comparables en el uso del dominio público radioeléctrico, pudiendo permitir la asignación de bloques similares de frecuencias radioeléctricas;

d) permanecerá abierto a otros Estados miembros de la Unión Europea en todo momento hasta que se haya realizado el proceso de asignación conjunta.

11. Los operadores que suministren las redes o servicios de comunicaciones electrónicas que hagan uso del dominio público radioeléctrico deberán disponer del correspondiente título habilitante de dicho uso.

Los operadores que vayan a efectuar materialmente emisiones radioeléctricas mediante el uso del dominio público radioeléctrico por encargo de otras personas o entidades deberán verificar, previamente al inicio de dichas emisiones, que las entidades a cuya disposición ponen su red ostentan el correspondiente título habilitante en materia de uso del dominio público radioeléctrico. Dichos operadores no podrán poner a disposición de las entidades referidas su red y, en consecuencia, no podrán dar el acceso a su red a dichas entidades ni podrán efectuar las mencionadas emisiones en caso de ausencia del citado título habilitante.

Los titulares de las infraestructuras físicas desde las que los operadores vayan a efectuar materialmente emisiones radioeléctricas mediante el uso del dominio público radioeléctrico, ya sea directamente o mediante acuerdos de coubicación, deberán tener identificada la titularidad de cada uno de los transmisores instalados susceptibles de producir emisiones radioeléctricas y una relación actualizada de las frecuencias utilizadas por cada transmisor.

Artículo 89. *Títulos habilitantes otorgados mediante un procedimiento de licitación.*

1. Cuando sea preciso para garantizar el uso eficaz y eficiente del dominio público radioeléctrico, teniendo debidamente en cuenta la necesidad de conseguir los máximos beneficios para los usuarios y facilitar el desarrollo de la competencia, el Ministerio de Asuntos Económicos y Transformación Digital podrá, previa consulta pública a las partes interesadas, incluidas las asociaciones de consumidores y usuarios, por un plazo de treinta días naturales y previo informe de la Comisión Nacional de los Mercados y la Competencia, limitar el número de concesiones demaniales a otorgar sobre dicho dominio para el suministro de redes públicas y la prestación de servicios de comunicaciones electrónicas. Toda decisión de limitar el otorgamiento de derechos de uso habrá de ser publicada, exponiendo los motivos de la misma. La limitación del número de títulos habilitantes será revisable por el propio Ministerio, de oficio o a instancia de parte, en la medida en que desaparezcan las causas que la motivaron.

2. Cuando, de conformidad con lo previsto en el apartado anterior, el titular del Ministerio de Asuntos Económicos y Transformación Digital limite el número de concesiones demaniales a otorgar en una determinada banda de frecuencias, se tramitará un procedimiento de licitación para el otorgamiento de las mismas que respetará en todo caso los principios de publicidad, concurrencia y no discriminación para todas las partes interesadas. Para ello se aprobará, mediante orden del titular del Ministerio de Asuntos Económicos y Transformación Digital, la convocatoria y el pliego de bases por el que se regirá la licitación, previa consulta pública por un plazo no inferior a treinta días naturales y previo informe de la Comisión Nacional de los Mercados y la Competencia.

Los objetivos que pueden perseguirse con la convocatoria de la licitación deberán limitarse a uno o varios de los siguientes:

a) fomentar la competencia;
b) promover la cobertura;
c) asegurar la calidad del servicio requerida;
d) fomentar el uso eficiente del dominio público radioeléctrico teniendo en cuenta, en particular, las condiciones asociadas a los derechos de uso y la cuantía de las tasas;
e) promover la innovación y el desarrollo de las empresas.

Antes de la convocatoria de la licitación, el Ministerio de Asuntos Económicos y Transformación Digital informará al RSPG de la próxima convocatoria y determinará si solicita al RSPG que convoque un foro de revisión por pares a fin de debatir y cambiar impresiones sobre la licitación y facilitar el intercambio de experiencias y buenas prácticas.

El procedimiento de licitación deberá resolverse mediante orden del titular del Ministerio de Asuntos Económicos y Transformación Digital en un plazo máximo de ocho meses desde la convocatoria de la licitación.

Artículo 90. *Competencia efectiva en la asignación y uso del dominio público radioeléctrico.*

1. Se promoverá una competencia efectiva y se evitará el falseamiento de la competencia cuando se tomen decisiones referentes a la asignación o modificación de los derechos de uso del dominio público radioeléctrico.

2. A tal efecto, en el Cuadro Nacional de Atribución de Frecuencias o en los pliegos reguladores de los procedimientos de licitación para el otorgamiento de títulos habilitantes se podrán tomar las siguientes medidas, previo informe de la Comisión Nacional de los Mercados y la Competencia:

a) establecer cautelas para evitar comportamientos especulativos o acaparamiento de derechos de uso del dominio público radioeléctrico, en particular, mediante la fijación de límites en la cantidad de frecuencias a utilizar por un mismo operador o grupo empresarial o la fijación de plazos estrictos para la explotación de los derechos de uso por parte de su titular, pudiendo establecer un período de tiempo durante el cual no se pueden efectuar operaciones de mercado secundario con los títulos habilitantes o los derechos de uso del dominio público radioeléctrico;

b) imponer condiciones a la concesión de tales derechos, como podría ser el suministro de acceso al por mayor, o la itinerancia nacional o inferior, en determinadas bandas o grupos de bandas con características similares;

c) reservar, si resulta conveniente y justificado debido a una situación específica del mercado, una parte de una banda del dominio público radioeléctrico o grupo de bandas para su asignación a nuevos operadores en el mercado.

3. Asimismo, el Ministerio de Asuntos Económicos y Transformación Digital podrá adoptar las siguientes medidas, previo informe de la Comisión Nacional de los Mercados y la Competencia:

a) denegar la concesión de nuevos derechos del uso del dominio público radioeléctrico o la de nuevos usos de dicho dominio público en determinadas bandas, o imponer condiciones a la concesión de nuevos derechos de uso del dominio público radioeléctrico o a la autorización de nuevos usos de dicho dominio público, con el fin de evitar un falseamiento de la competencia por efecto de asignaciones, transferencias o acumulaciones de derechos de uso;

b) incluir condiciones que prohíban las transferencias de derechos de uso del dominio público no sujetos a la normativa de control de fusiones, o impongan condiciones a las mismas, si tales transferencias pudieran ser perjudiciales para la competencia;

c) modificar los derechos de uso del dominio público radioeléctrico si fuera necesario para poner remedio a posteriori a falseamientos de la competencia causados por la transferencia o acumulación de derechos de uso del espectro radioeléctrico.

4. La adopción por el Ministerio de Asuntos Económicos y Transformación Digital de las medidas a las que se refiere este artículo se basará en una evaluación objetiva y prospectiva de las condiciones de competencia del mercado y de si tales medidas son necesarias para lograr o mantener una competencia efectiva, y de los efectos previsibles de las mismas sobre la inversión presente y futura de los agentes del mercado, especialmente por lo que se refiere al despliegue de las redes. Al hacerlo, tendrá en cuenta el enfoque del análisis del mercado expuesto en los apartados 1 a 3 del artículo 17.

Artículo 91. *Condiciones asociadas a los títulos habilitantes para el uso del dominio público radioeléctrico.*

1. Cuando se otorgue un título habilitante para el uso del dominio público radioeléctrico, se especificará su duración, sus causas de extinción y revocación y si los derechos de uso pueden ser objeto de operaciones de mercado secundario y sus condiciones.

2. En el otorgamiento de los títulos habilitantes, el Ministerio de Asuntos Económicos y Transformación Digital, previo informe de la Comisión Nacional de los Mercados y la Competencia, podrá imponer las siguientes condiciones para garantizar un uso eficaz y eficiente del dominio público radioeléctrico o reforzar la cobertura:

a) compartir infraestructuras pasivas o activas dependientes del dominio público radioeléctrico, o compartir el dominio público radioeléctrico;

b) celebrar acuerdos comerciales de acceso por itinerancia nacional o inferior;

c) desplegar conjuntamente infraestructuras para el suministro de redes o servicios que dependen del uso del dominio público radioeléctrico.

3. Los operadores de redes públicas de comunicaciones electrónicas o de servicios de comunicaciones electrónicas disponibles al público podrán permitir un acceso público a sus redes a través de RLAN que podrían estar situadas en los locales de un usuario final, siempre que se atengan a las condiciones establecidas en este título y al acuerdo previo y con conocimiento de causa del usuario final.

4. Los operadores de redes públicas de comunicaciones electrónicas o de servicios de comunicaciones electrónicas disponibles al público no podrán restringir o impedir unilateralmente la posibilidad de que los usuarios:

a) accedan a las RLAN que prefieran suministradas por terceros, o

b) permitan el acceso recíproco o más en general a las redes de tales proveedores por parte de otros usuarios finales a través de redes de área local radioeléctricas, también si se trata de iniciativas de terceros que agregan y permiten el acceso público a las RLAN de diferentes usuarios finales.

5. Se permite que los usuarios finales permitan el acceso de forma recíproca o de otra forma a sus RLAN por parte de otros usuarios finales, también si se trata de iniciativas de terceros que agregan y permiten un acceso público a las RLAN de diferentes usuarios finales.

6. En los términos que se determinen reglamentariamente, con carácter previo a la utilización del dominio público radioeléctrico, se exigirá, preceptivamente, la aprobación del proyecto técnico o la presentación de una declaración responsable de conformidad con lo establecido en el artículo 69 de la Ley 39/2015, de 1 de octubre, del Procedimiento Común de las Administraciones públicas, así como la inspección de las instalaciones o una certificación expedida por técnico competente con el fin de comprobar que las instalaciones se ajustan a las condiciones previamente autorizadas.

En función de la naturaleza del servicio, de la banda de frecuencias empleada, de la importancia técnica de las instalaciones que se utilicen o por razones de eficacia en la gestión del espectro, se determinarán los supuestos en los que procede la exigencia de presentación o aprobación de proyecto técnico o una declaración responsable de conformidad con lo establecido en el artículo 69 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, sin perjuicio de que la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales pueda exigir en cualquier momento la presentación del proyecto técnico. Asimismo, también se determinarán los supuestos en los que procede la inspección previa o una certificación expedida por técnico competente.

Artículo 92. *Uso compartido.*

1. El Ministerio de Asuntos Económicos y Transformación Digital, previo informe de la Comisión Nacional de los Mercados y la Competencia, podrá imponer a los operadores de redes públicas de comunicaciones electrónicas obligaciones en relación con la compartición de la infraestructura pasiva u obligaciones para celebrar acuerdos de acceso itinerante localizado, siempre que, en ambos casos, ello resulte directamente necesario para la prestación local de servicios que dependen de la utilización del dominio público radioeléctrico, de conformidad con lo dispuesto en la presente ley y su normativa de desarrollo, y siempre que los operadores no dispongan de medios de acceso alternativos viables y similares para los usuarios finales en el marco de unas condiciones justas y razonables.

2. El Ministerio de Asuntos Económicos y Transformación Digital podrá excepcionalmente imponer tales obligaciones únicamente si esta posibilidad se ha establecido claramente en el momento de otorgar el título habilitante de derechos de uso del dominio público y si ello está justificado por el hecho de que, en la zona sujeta a tales obligaciones, el despliegue de infraestructuras con base en el mercado para el suministro de redes o servicios que dependan del uso del dominio público radioeléctrico esté sujeto a obstáculos físicos o económicos insalvables, y el acceso a las redes o los servicios por parte de los usuarios finales sea, por consiguiente, muy deficiente o inexistente.

3. Cuando el acceso itinerante localizado y el uso compartido de la infraestructura pasiva no basten para abordar la situación, la Comisión Nacional de los Mercados y la Competencia

podrá imponer obligaciones relativas al uso compartido de la infraestructura activa si esta posibilidad se ha establecido claramente en el momento de otorgar el título habilitante de derechos de uso del dominio público.

4. El Ministerio de Asuntos Económicos y Transformación Digital y la Comisión Nacional de los Mercados y la Competencia, al imponer estas obligaciones de uso compartido, tomará en consideración:

a) la necesidad de maximizar la conectividad a lo largo de los principales corredores de transporte y en áreas territoriales particulares;

b) la posibilidad de aumentar considerablemente las posibilidades de elección y una mejor calidad de servicio para los usuarios finales;

c) el uso eficiente del dominio público radioeléctrico;

d) la viabilidad técnica de la compartición y las condiciones conexas;

e) el estado de la competencia basada en las infraestructuras, así como el de la competencia basada en los servicios;

f) la innovación tecnológica;

g) la necesidad imperativa de incentivar al operador anfitrión para desplegar la infraestructura en el primer lugar.

5. En caso de resolución de conflictos, la Comisión Nacional de los Mercados y la Competencia podrá imponer al beneficiario de la obligación de compartición o acceso, entre otras, la obligación de compartir el espectro radioeléctrico con la infraestructura de acogida en la zona de que se trate.

Artículo 93. *Neutralidad tecnológica y de servicios en el uso del dominio público radioeléctrico.*

1. En las bandas de radiofrecuencias declaradas disponibles para los servicios de comunicaciones electrónicas en el Cuadro Nacional de Atribución de Frecuencias se podrá emplear cualquier tipo de tecnología utilizada para los servicios de comunicaciones electrónicas de conformidad con el Derecho de la Unión Europea.

Podrán, no obstante, preverse restricciones proporcionadas y no discriminatorias a los tipos de tecnología de acceso inalámbrico o red radioeléctrica utilizados para los servicios de comunicaciones electrónicas cuando sea necesario para:

a) evitar interferencias perjudiciales;

b) proteger la salud pública frente a los campos electromagnéticos;

c) asegurar la calidad técnica del servicio;

d) garantizar un uso compartido máximo de las radiofrecuencias;

e) garantizar un uso eficiente del espectro;

f) garantizar el logro de un objetivo de interés general.

2. En las bandas de radiofrecuencias declaradas disponibles para los servicios de comunicaciones electrónicas en el Cuadro Nacional de Atribución de Frecuencias se podrá prestar cualquier tipo de servicios de comunicaciones electrónicas, de conformidad con el Derecho de la Unión Europea.

Podrán, no obstante, preverse restricciones proporcionadas y no discriminatorias a los tipos de servicios de comunicaciones electrónicas que se presten, incluido, cuando proceda, el cumplimiento de un requisito del Reglamento de Radiocomunicaciones de la Unión Internacional de Telecomunicaciones.

Las medidas que exijan que un servicio de comunicaciones electrónicas se preste en una banda específica disponible para los servicios de comunicaciones electrónicas deberán estar justificadas para garantizar el logro de objetivos de interés general definidos con arreglo al Derecho de la Unión Europea, tales como:

a) la seguridad de la vida humana;

b) la promoción de la cohesión social, regional o territorial;

c) la evitación del uso ineficiente de las radiofrecuencias;

d) la promoción de la diversidad cultural y lingüística y del pluralismo de los medios de comunicación, mediante, por ejemplo, la prestación de servicios de comunicación audiovisual televisivos y radiofónicos.

Únicamente se impondrá la atribución específica de una banda de frecuencias para la prestación de un determinado servicio de comunicaciones electrónicas cuando esté justificado por la necesidad de proteger servicios relacionados con la seguridad de la vida o, excepcionalmente, cuando sea necesario para alcanzar objetivos de interés general definidos con arreglo al Derecho de la Unión Europea.

3. Las restricciones a la utilización de bandas de frecuencias que, en su caso, se establezcan de conformidad con los apartados anteriores sólo podrán adoptarse tras haber dado a las partes interesadas la oportunidad de formular observaciones sobre la medida propuesta, en un plazo razonable.

4. Periódicamente, la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales revisará la pertinencia de mantener las restricciones a la utilización de bandas de frecuencias que, en su caso, se establezcan de conformidad con los apartados anteriores, hará públicos los resultados de estas revisiones y elevará las propuestas correspondientes al órgano competente para su aprobación.

Artículo 94. *Duración de los títulos habilitantes para el uso del dominio público radioeléctrico.*

1. Los derechos de uso privativo del dominio público radioeléctrico sin limitación de número se otorgarán, con carácter general, por un período que finalizará el 31 de diciembre del año natural en que cumplan su quinto año de vigencia, renovables por períodos de cinco años en función de las disponibilidades y previsiones de la planificación de dicho dominio público. La renovación no podrá otorgar ventajas indebidas a su titular. Mediante real decreto se determinarán los supuestos en los que podrá fijarse un período de duración distinto para los derechos de uso privativo del dominio público radioeléctrico sin limitación de número.

2. Los derechos de uso privativo con limitación de número tendrán la duración prevista en los correspondientes procedimientos de licitación. A la hora de determinar en el procedimiento de licitación la duración concreta de los derechos de uso, se tendrán en cuenta, entre otros criterios, la necesidad de garantizar la competencia, un uso eficaz y eficiente del dominio público radioeléctrico y de promover la innovación y las inversiones eficientes, incluso autorizando un período apropiado de amortización de las inversiones, las obligaciones vinculadas a los derechos de uso, como la cobertura mínima que se imponga, y las bandas de frecuencias cuyos derechos de uso se otorguen, en los términos que se concreten mediante real decreto.

3. Los derechos de uso privativo con limitación de número tendrán la duración mínima de veinte años.

En el caso de que resulte necesario para incentivar la inversión eficiente y rentable en infraestructuras, los derechos de uso privativo con limitación de número podrán ser objeto de una prórroga, por una sola vez, por una duración mínima de cinco años y una duración máxima de veinte años adicionales. La duración concreta de la prórroga se determinará en el pliego regulador de la licitación.

4. Los criterios concretos para el otorgamiento de la prórroga se determinarán en el pliego regulador de la licitación y se basarán en alguno de los siguientes criterios generales:

a) el uso eficaz y eficiente del dominio público radioeléctrico de que se trate;
b) el cumplimiento de objetivos de cobertura territorial y de población;
c) el cumplimiento de objetivos de alta calidad y velocidad;
d) el cumplimiento de objetivos de cobertura de los grandes corredores de transporte;
e) las aportaciones al desarrollo de nuevas tecnologías y aplicaciones inalámbricas;
f) el cumplimiento de objetivos de interés general de protección de la seguridad de la vida humana;
g) el cumplimiento de objetivos de interés general de protección del orden público, la seguridad pública o la seguridad nacional;
h) el cumplimiento de cualquier compromiso asumido en el procedimiento de licitación;
i) la necesidad de garantizar una competencia no falseada.

5. El Ministerio de Asuntos Económicos y Transformación Digital, antes del plazo de dos años a contar desde la fecha de finalización del período de vigencia inicial del título

habilitante, realizará una evaluación objetiva de los criterios concretos para el otorgamiento de la prórroga determinados en el pliego regulador de la licitación.

Los interesados dispondrán de un plazo de tres meses para presentar alegaciones en el expediente de prórroga del título habilitante.

Partiendo de dicha evaluación, el Ministerio de Asuntos Económicos y Transformación Digital, previo informe de la Comisión Nacional de los Mercados y la Competencia, decidirá sobre el otorgamiento de la prórroga.

6. Se podrán establecer unos plazos de duración mínimos y máximos diferentes a los previstos anteriormente cuando esté debidamente justificado en los siguientes casos:

a) en zonas geográficas limitadas en las que el acceso a redes de alta capacidad sea muy deficiente o inexistente;

b) para proyectos específicos a corto plazo;

c) para uso experimental;

d) para aquellos usos del dominio público radioeléctrico que, de conformidad con los principios de neutralidad tecnológica y de servicios, puedan coexistir con servicios de banda ancha inalámbrica;

e) para usos alternativos del espectro radioeléctrico, de conformidad con lo dispuesto en el artículo 88.7;

f) para ajustar la duración de los derechos de uso del dominio público radioeléctrico en aras de garantizar la expiración simultánea de la duración de los derechos en una o varias bandas de frecuencias.

7. Salvo que en los correspondientes procedimientos de licitación se haya previsto que no pueden ser objeto de renovación, los derechos de uso privativo con limitación de número podrán ser renovados antes del término de su duración.

En los casos en que esté permitido, el Ministerio de Asuntos Económicos y Transformación Digital evaluará la necesidad de renovar por iniciativa propia o a petición del titular de los derechos, en cuyo caso la renovación no tendrá lugar antes de los cinco años de su término.

Al analizar una eventual renovación, el Ministerio de Asuntos Económicos y Transformación Digital, llevará a cabo un procedimiento abierto, transparente y no discriminatorio, y, en particular:

a) dará a todas las partes interesadas la oportunidad de manifestar su punto de vista a través de un procedimiento público de consulta conforme con lo dispuesto en la disposición adicional décima, y

b) expondrá claramente las razones de la eventual renovación.

El Ministerio de Asuntos Económicos y Transformación Digital deberá tener en cuenta cualquier constatación en el seno del procedimiento público de consulta mencionado de que existe una demanda de mercado procedente de empresas diferentes de los titulares de los derechos de uso de la banda considerada del espectro radioeléctrico al decidir si renueva los derechos de uso u organiza un nuevo procedimiento de licitación.

Toda decisión de renovación podrá ir acompañada de una revisión de las condiciones asociadas al título habilitante.

Artículo 95. *Modificación, extinción y revocación de los títulos habilitantes para el uso del dominio público radioeléctrico.*

1. Con arreglo a los principios de objetividad y de proporcionalidad, atendiendo principalmente a las necesidades de la planificación y del uso eficiente y a la disponibilidad del espectro radioeléctrico, en los términos establecidos mediante real decreto, el Ministerio de Asuntos Económicos y Transformación Digital podrá modificar los títulos habilitantes para el uso del dominio público radioeléctrico, previa audiencia del interesado.

En el caso de que se trate de títulos habilitantes que hubiesen sido otorgados por el procedimiento de licitación, y salvo cuando se trate de propuestas de modificación de escasa importancia convenidas con el titular de los derechos de uso del dominio público radioeléctrico, la propuesta de modificación deberá requerir el informe previo de la Comisión Nacional de los Mercados y la Competencia y audiencia del Consejo de Consumidores y

Usuarios y, en su caso, de las asociaciones más representativas de los restantes usuarios durante un plazo suficiente, que, salvo en circunstancias excepcionales, no podrá ser inferior a cuatro semanas. En estos casos la modificación se realizará mediante orden ministerial, previo informe de la Comisión Delegada del Gobierno para Asuntos Económicos, que establecerá un plazo para que los titulares se adapten a ella.

La modificación de los títulos habilitantes para el uso del dominio público radioeléctrico, en los casos en que justificadamente haya que establecer condiciones distintas a las que existían cuando se otorgó el título, podrá consistir en prolongar la duración de derechos ya existentes, incluso más allá de las duraciones establecidas en el artículo anterior.

2. Los títulos habilitantes para el uso del dominio público se extinguirán por:

a) las causas que resulten aplicables de las reseñadas en el artículo 100 de la Ley 33/2003, de 3 de noviembre, de Patrimonio de las Administraciones públicas;

b) muerte del titular del derecho de uso del dominio público radioeléctrico o extinción de la persona jurídica titular;

c) renuncia del titular, con efectos desde su aceptación por el órgano competente del Ministerio de Asuntos Económicos y Transformación Digital;

d) pérdida de la condición de operador del titular del derecho de uso del dominio público radioeléctrico, cuando dicha condición fuera necesaria, o cualquier causa que imposibilite la prestación del servicio por su titular;

e) falta de pago de la tasa por reserva del dominio público radioeléctrico;

f) pérdida de adecuación de las características técnicas de la red al Cuadro Nacional de Atribución de Frecuencias, sin que exista posibilidad de otorgar al titular otras bandas;

g) mutuo acuerdo entre el titular y el órgano competente del Ministerio de Asuntos Económicos y Transformación Digital;

h) transcurso del tiempo para el que se otorgaron. En el caso de los derechos de uso sin limitación de número, por el transcurso del tiempo para el que se otorgaron sin que se haya efectuado su renovación;

i) por incumplimiento grave y reiterado de las obligaciones del titular contempladas como causa de revocación;

j) aquellas otras causas que se establezcan en el título habilitante, conforme a la presente ley.

3. El órgano competente del Ministerio de Asuntos Económicos y Transformación Digital, a través del procedimiento administrativo general de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, podrá acordar la revocación de los títulos habilitantes para el uso del dominio público radioeléctrico por las siguientes causas:

a) el incumplimiento de las condiciones y requisitos técnicos aplicables al uso del dominio público radioeléctrico;

b) no pagar el Impuesto de Transmisiones Patrimoniales y Actos Jurídicos Documentados;

c) no efectuar un uso eficaz o eficiente del dominio público radioeléctrico;

d) la utilización de las frecuencias con fines distintos a los que motivaron su asignación o para otros diferentes de los de la prestación del servicio o el ejercicio de la actividad que haya motivado su asignación, siempre que no sean aplicables algunas de las restricciones previstas en los apartados 1 o 2 del artículo 93.

Artículo 96. *Protección activa del dominio público radioeléctrico.*

1. La Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, en cualquier momento, podrá efectuar una protección activa del dominio público radioeléctrico mediante la realización de emisiones sin contenidos sustantivos en aquellas frecuencias y canales radioeléctricos cuyos derechos de uso, en el ámbito territorial correspondiente, no hayan sido otorgados.

Esta potestad se ejercitará sin perjuicio de las actuaciones inspectoras y sancionadoras que se puedan llevar a cabo para depurar las responsabilidades en que se hubieran podido incurrir por el uso del dominio público radioeléctrico sin disponer de título habilitante, por la

producción de interferencias o por la comisión de cualquier otra infracción tipificada en el marco del régimen sancionador establecido en el título VIII.

2. Mediante real decreto se regulará el procedimiento para el ejercicio de la potestad de protección activa del dominio público radioeléctrico en el caso de que la frecuencia o canal radioeléctrico sea objeto de una ocupación o uso efectivo sin que se disponga de título habilitante, con sujeción a las siguientes normas:

a) se constatará la ocupación o uso efectivo de la frecuencia o canal radioeléctrico sin que se disponga de título habilitante para ello;

b) se efectuará un trámite de previa audiencia a la persona física o jurídica que esté efectuando la ocupación o el uso de la frecuencia o canal radioeléctrico sin título habilitante o, en su caso, al titular de las infraestructuras, de la finca o del inmueble desde donde se produce la emisión en esa frecuencia, para que en el plazo de diez días hábiles alegue lo que estime oportuno;

c) en su caso, una vez efectuado el trámite de previa audiencia, se requerirá a la persona o titular mencionado anteriormente con el que se evacuó dicho trámite, para que en el plazo de ocho días hábiles proceda al cese de las emisiones no autorizadas;

d) en el caso de que no se proceda al cese de las emisiones no autorizadas, la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales podrá iniciar sus emisiones en dicha frecuencia o canal radioeléctrico.

Artículo 97. *Mercado secundario en el dominio público radioeléctrico.*

1. Los títulos habilitantes de uso del dominio público radioeléctrico podrán ser transferidos y los derechos de uso del dominio público radioeléctrico podrán ser objeto de cesión, utilización o mutualización, ya sea de forma total o parcial, en las condiciones de autorización que se establezcan mediante real decreto.

En dicho real decreto se identificarán igualmente las bandas de frecuencia en las que no se pueden efectuar operaciones de transferencia de títulos o cesión, utilización o mutualización de derechos de uso de dominio público radioeléctrico.

2. En el caso de la cesión, utilización o mutualización, en ningún caso se eximirá al titular del derecho de uso de las obligaciones asumidas frente a la Administración. Cualquier transferencia de título habilitante o cesión, utilización o mutualización de derechos de uso del dominio público radioeléctrico deberá en todo caso respetar las condiciones técnicas de uso establecidas en el Cuadro Nacional de Atribución de Frecuencias o en los planes técnicos o las que, en su caso, estén fijadas en las medidas técnicas de aplicación de la Unión Europea.

3. Mediante dicho real decreto se establecerán también las restricciones a la transferencia, cesión, utilización o mutualización de derechos individuales de uso de radiofrecuencias cuando dichos derechos se hubieran obtenido inicialmente de forma gratuita.

TÍTULO VI

La administración de las telecomunicaciones

Artículo 98. *Competencias de la Administración General del Estado y de sus organismos públicos.*

1. Tendrán la consideración de autoridades públicas competentes específicas en materia de telecomunicaciones:

a) los órganos superiores y directivos del Ministerio de Asuntos Económicos y Transformación Digital que, de conformidad con la estructura orgánica del departamento, asuman las competencias asignadas a este ministerio en materias reguladas por esta ley;

b) la Comisión Nacional de los Mercados y la Competencia en el ejercicio de las competencias que se le han asignado en materias reguladas por esta ley. En el ejercicio de estas competencias, tiene la consideración de autoridad nacional de reglamentación a los efectos del Código Europeo de Comunicaciones Electrónicas.

2. En el desarrollo de las competencias que tengan encomendadas, dichas autoridades cooperarán mutuamente, con los restantes órganos competentes de otros Estados miembros y con los organismos pertinentes de la Unión Europea, a fin de fomentar la aplicación coherente de la normativa comunitaria en materia de comunicaciones electrónicas y contribuir al desarrollo del mercado interior. Con tal fin, apoyarán activamente los objetivos de la Comisión y del Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (ORECE) de promover una mayor coordinación, en particular, teniendo en cuenta en la medida de lo posible las recomendaciones de armonización de la Comisión Europea. Asimismo, colaborarán con ambas instituciones, a fin de determinar qué tipos de instrumentos y soluciones son los más apropiados para tratar situaciones particulares de mercado.

3. En el desarrollo de las competencias que tengan encomendadas, dichas autoridades, deberán tener en cuenta en la mayor medida posible los objetivos enunciados en el artículo 3 y aplicarán principios reguladores objetivos, transparentes, no discriminatorios y proporcionados, con arreglo a los siguientes fines y criterios:

a) promover un entorno regulador previsible, garantizando un enfoque regulador coherente en períodos de revisión apropiados;

b) fomentar la inversión eficiente orientada al mercado y la innovación en infraestructuras nuevas y mejoradas, incluso asegurando que toda obligación relativa al acceso tenga debidamente en cuenta los riesgos en que incurren las empresas inversoras, y permitir diferentes modalidades de cooperación entre los inversores y las partes que soliciten el acceso, con el fin de diversificar el riesgo de las inversiones y velar por que se respeten la competencia en el mercado y el principio de no discriminación;

c) imponer obligaciones específicas únicamente cuando no exista una competencia efectiva y sostenible, y suprimir dichas obligaciones en cuanto se constate el cumplimiento de dicha condición;

d) garantizar que, en circunstancias similares, no se dispense un trato discriminatorio a las empresas suministradoras de redes y servicios de comunicaciones electrónicas;

e) salvaguardar la competencia en beneficio de los consumidores y promover, cuando sea posible, la competencia basada en las infraestructuras, especialmente mediante la instalación y explotación de redes de alta y muy alta capacidad;

f) tener debidamente en cuenta la variedad de condiciones en cuanto a la competencia y los consumidores que existen en las distintas regiones geográficas;

g) ejercer sus responsabilidades de tal modo que se promueva la eficiencia, la competencia sostenible y el máximo beneficio para los usuarios finales.

Artículo 99. *Ministerio de Asuntos Económicos y Transformación Digital.*

Los órganos superiores y directivos del Ministerio de Asuntos Económicos y Transformación Digital que, de conformidad con la estructura orgánica del departamento, asuman las competencias asignadas a este ministerio, ejercerán las siguientes funciones:

a) ejecutar la política adoptada por el Gobierno en los servicios de telecomunicaciones para la seguridad nacional, la defensa nacional, la seguridad pública, la seguridad vial y la protección civil a los que se refiere el artículo 4;

b) ejercer las competencias que en materia de acceso a las redes y recursos asociados, interoperabilidad e interconexión le atribuye la presente ley y su desarrollo reglamentario, en particular, en los siguientes supuestos:

1.º en los procedimientos de licitación para la obtención de derechos de uso del dominio público radioeléctrico;

2.º cuando se haga necesario para garantizar el cumplimiento de la normativa sobre datos personales y protección de la intimidad en el sector de las comunicaciones electrónicas;

3.º cuando resulte preciso para garantizar el cumplimiento de compromisos internacionales en materia de telecomunicaciones;

c) imponer obligaciones a los operadores de comunicaciones electrónicas que controlen el acceso a los usuarios finales para que sus servicios sean interoperables, en los términos indicados en el artículo 14.6;

d) imponer obligaciones a los operadores de servicios de comunicaciones interpersonales independientes de la numeración para que sus servicios sean interoperables, cuando la conectividad de extremo a extremo entre usuarios finales esté en peligro debido a una falta de interoperabilidad entre los servicios de comunicaciones interpersonales, y en la medida en que sea necesario para garantizar la conectividad de extremo a extremo entre usuarios finales, en los términos indicados en el artículo 14.6;

e) proponer al Gobierno la aprobación de los planes nacionales de numeración y llevar a cabo la atribución de los derechos de uso de los recursos públicos regulados en dichos planes y ejercer las demás competencias que le atribuye el capítulo VII del título II;

f) proponer al Gobierno la política a seguir para facilitar el desarrollo y la evolución de las obligaciones de servicio público a las que se hace referencia en el capítulo I del título III y la desarrollará asumiendo la competencia de control y seguimiento de las obligaciones de servicio público que correspondan a los distintos operadores en la explotación de redes o la prestación de servicios de comunicaciones electrónicas;

g) proponer al Gobierno la política a seguir para reconocer y garantizar los derechos y obligaciones de carácter público en la explotación de redes y en la prestación de servicios de comunicaciones electrónicas, así como los derechos de los usuarios finales a los que se hace referencia en los capítulos II, III y IV del título III;

h) verificar el cumplimiento de los requisitos, acuerdos y las condiciones establecidas en el artículo 76 para garantizar el derecho de los usuarios finales de acceso abierto a internet y publicar el informe anual al que se refiere dicho artículo;

i) verificar el cumplimiento de los requisitos y las condiciones establecidas en el Reglamento (UE) 531/2012 del Parlamento Europeo y del Consejo, de 13 de junio de 2012, relativo a la itinerancia en las redes públicas de comunicaciones móviles en la Unión, en materia de acceso de los usuarios finales a los servicios de comunicaciones electrónicas de voz, SMS y datos en itinerancia en la Unión Europea, incluida su venta por separado, la correcta prestación de servicios regulados de itinerancia al por menor, la correcta aplicación de las tarifas al por menor de servicios regulados de itinerancia, la no inclusión de recargos y de sus condiciones y mecanismos de transparencia, así como la correcta aplicación por los operadores de itinerancia de su política de utilización razonable al consumo de servicios regulados de itinerancia al por menor, la resolución de controversias entre usuarios finales y operadores por la prestación de servicios de itinerancia y el control y supervisión de la itinerancia involuntaria en zonas fronterizas;

j) verificar la correcta aplicación de las tarifas al por menor de las comunicaciones intracomunitarias reguladas en los términos establecidos en el Reglamento (UE) 2015/2120 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015, a excepción de la materia relativa a la sostenibilidad del modelo de tarificación nacional de un operador;

k) gestionar el Registro de empresas instaladoras de telecomunicación;

l) formular las propuestas para la elaboración de normativa relativa a las infraestructuras comunes de comunicaciones electrónicas en el interior de edificios y conjuntos inmobiliarios, y el seguimiento de su implantación en España;

m) ejercer las funciones en materia de acceso a infraestructuras susceptibles de alojar redes públicas de comunicaciones electrónicas, de coordinación de obras civiles y de acceso o uso de las redes de comunicaciones electrónicas titularidad de los órganos o entes gestores de infraestructuras de transporte de competencia estatal a que se refieren los artículos 52 a 54, salvo la resolución de conflictos;

n) ejercer las funciones en materia de requisitos esenciales y evaluación de conformidad de equipos de telecomunicación a las que se refiere el título IV;

ñ) ejercer las funciones en materia de administración del dominio público radioeléctrico a las que se refiere el título V. En particular, ejercerá las siguientes funciones:

1.º la propuesta de planificación, la gestión y el control del dominio público radioeléctrico, así como la tramitación y el otorgamiento de los títulos habilitantes para su utilización;

2.º el ejercicio de las funciones atribuidas a la Administración General del Estado en materia de autorización e inspección de instalaciones radioeléctricas en relación con los niveles únicos de emisión radioeléctrica permitidos a que se refiere el artículo 86.b);

3.º la gestión de un registro público de radiofrecuencias, accesible a través de internet, en el que constarán los titulares de concesiones administrativas para el uso privativo del dominio público radioeléctrico;

4.º la elaboración de proyectos y desarrollo de los planes técnicos nacionales de radiodifusión y televisión;

5.º la comprobación técnica de emisiones radioeléctricas para la identificación, localización y eliminación de interferencias perjudiciales, infracciones, irregularidades y perturbaciones de los sistemas de radiocomunicación, y la verificación del uso efectivo y eficiente del dominio público radioeléctrico por parte de los titulares de derechos de uso;

6.º la protección del dominio público radioeléctrico, para lo cual podrá, entre otras actuaciones, realizar emisiones en aquellas frecuencias y canales radioeléctricos cuyos derechos de uso, en el ámbito territorial correspondiente, no hayan sido otorgados;

7.º la gestión de la asignación de los recursos órbita-espectro para comunicaciones por satélite;

8.º la elaboración de estudios e informes y, en general, el asesoramiento de la Administración General del Estado en todo lo relativo a la administración del dominio público radioeléctrico;

9.º la participación en los organismos internacionales relacionados con la planificación, gestión y control del espectro radioeléctrico.

o) gestionar en período voluntario las tasas en materia de telecomunicaciones a que se refiere la presente ley que no correspondan a la Comisión Nacional de los Mercados y la Competencia;

p) controlar el cumplimiento de las condiciones que sobre el suministro de redes públicas y prestación de servicios de comunicaciones electrónicas en régimen de prestación a terceros por las Administraciones públicas vienen establecidas en el artículo 13;

q) realizar las funciones atribuidas de manera expresa por la normativa comunitaria, la presente ley y su normativa de desarrollo;

r) realizar cualesquiera otras funciones que le sean atribuidas por ley o por real decreto.

Artículo 100. *La Comisión Nacional de los Mercados y la Competencia.*

1. La naturaleza, funciones, estructura, personal, presupuesto y demás materias que configuran la Comisión Nacional de los Mercados y la Competencia están reguladas en la Ley 3/2013, de 4 de junio, de creación de la Comisión Nacional de los Mercados y la Competencia.

2. En particular, en las materias reguladas por la presente ley, la Comisión Nacional de los Mercados y la Competencia ejercerá las siguientes funciones:

a) definir y analizar los mercados de referencia relativos a redes y servicios de comunicaciones electrónicas y el ámbito geográfico de los mismos, cuyas características pueden justificar la imposición de obligaciones específicas, en los términos establecidos en los artículos 15 y 16 y su normativa de desarrollo;

b) identificar el operador u operadores que poseen un peso significativo en el mercado cuando del análisis de los mercados de referencia se constate que no se desarrollan en un entorno de competencia efectiva;

c) establecer, cuando proceda, las obligaciones específicas que correspondan a los operadores con peso significativo en mercados de referencia, incluidos los operadores exclusivamente mayoristas, en los términos establecidos en el capítulo III del título II y su normativa de desarrollo;

d) decidir la imposición, como medida excepcional, a los operadores con peso significativo en el mercado integrados verticalmente, de la obligación de separación funcional de acuerdo con los requisitos y procedimientos indicados en el artículo 25;

e) imponer obligaciones de interconexión de redes a los operadores que controlen el acceso a los usuarios finales, en la medida en que sea necesario garantizar la posibilidad de conexión de extremo a extremo, en los términos indicados en el artículo 14.7;

f) imponer obligaciones a los operadores para que faciliten acceso a los interfaces de programa de aplicaciones (API) y guías electrónicas de programación (EPG), en condiciones justas, razonables y no discriminatorias. en la medida en que sea necesario para garantizar el acceso de los usuarios finales a los servicios digitales de comunicación audiovisual televisivos y radiofónicos y los servicios complementarios conexos, en los términos indicados en el artículo 14.7;

g) adoptar decisiones por las que otorgue carácter vinculante a los compromisos que en materia de acceso y coinversión, incluyendo las redes de muy alta capacidad, hayan sido ofrecidos por los operadores con peso significativo en el mercado, así como asumir el control y supervisión de las mismas y velar por la ejecución de los compromisos a los que haya otorgado carácter vinculante;

h) velar por la adecuación y el cumplimiento del proceso de migración desde una infraestructura heredada que quieran realizar operadores que hayan sido declarados con peso significativo en uno o varios mercados pertinentes, consistente en el desmantelamiento y cierre o sustitución de partes de la red por una infraestructura nueva;

i) evaluar y, en su caso, imponer tarifas máximas de terminación de llamadas de voz en redes fijas y en redes móviles, o ambas, así como supervisar y velar por el cumplimiento de la aplicación de las tarifas de terminación de llamadas de voz establecidas a escala europea, en los términos establecidos en el artículo 23;

j) resolver los conflictos en los mercados de comunicaciones electrónicas a los que se refieren los artículos 28 y 29 y la Ley 3/2013, de 4 de junio, de creación de la Comisión Nacional de los Mercados y la Competencia.

En particular, le corresponderá resolver conflictos entre operadores relativos a la determinación de las condiciones concretas para la puesta en práctica de la obligación impuesta por el Ministerio de Asuntos Económicos y Transformación Digital de la utilización compartida del dominio público o la propiedad privada, o de la ubicación compartida de infraestructuras y recursos asociados, de acuerdo con el procedimiento regulado en el artículo 46, así como resolver conflictos sobre el acceso a infraestructuras susceptibles de alojar redes públicas de comunicaciones electrónicas, la coordinación de obras civiles y el acceso o uso de las redes de comunicaciones electrónicas titularidad de los órganos o entes gestores de infraestructuras de transporte de competencia estatal, en los términos establecidos por los artículos 52 a 54;

k) fijar las características y condiciones para garantizar el cambio de operador y la conservación de los números, así como el cambio de proveedor de los servicios de acceso a internet, en aplicación de los aspectos técnicos y administrativos que mediante real decreto se establezcan para que ésta se lleve a cabo;

l) determinar si la obligación de la prestación del servicio universal puede implicar una carga injusta para los operadores obligados a su prestación, así como determinar la cuantía que supone el coste neto en la prestación del servicio universal, a que se refiere al artículo 42;

m) definir y revisar la metodología para determinar el coste neto del servicio universal, tanto en lo que respecta a la imputación de costes como a la atribución de ingresos, que deberá basarse en procedimientos y criterios objetivos, transparentes, no discriminatorios y proporcionales y tener carácter público;

n) establecer el procedimiento para cuantificar los beneficios no monetarios obtenidos por el operador u operadores encargados de la prestación del servicio universal;

ñ) determinar las aportaciones que correspondan a cada uno de los operadores con obligaciones de contribución a la financiación del servicio universal y la gestión del Fondo nacional del servicio universal;

o) supervisar la evolución y el nivel de la tarificación al público de los servicios incluidos en el servicio universal de telecomunicaciones y garantizar la asequibilidad del servicio universal de telecomunicaciones, en coordinación con el Ministerio de Asuntos Económicos y Transformación Digital;

p) determinar los parámetros de calidad de servicio que habrán de cuantificarse y los métodos de medición aplicables, así como el contenido y formato de la información que deberá hacerse pública, incluidos posibles mecanismos de certificación de la calidad;

q) suministrar gratuitamente a las entidades mencionadas en el artículo 72, los datos sobre números de abonados que le faciliten los operadores de comunicaciones electrónicas, así como imponer obligaciones y condiciones a las empresas que controlan el acceso a los usuarios finales para que éstos puedan acceder a los servicios de información sobre números de abonados;

r) imponer obligaciones relativas al acceso o utilización compartida del cableado y recursos asociados de los tramos finales de las redes de acceso en el interior de los edificios o hasta el primer punto de concentración o distribución, o más allá del primer punto de concentración o distribución, en los términos indicados en el artículo 55.8;

s) determinar la localización del punto de terminación de la red;

t) asesorar sobre la configuración del mercado y sobre elementos relativos a la competencia en los procesos de otorgamiento de los derechos de uso del dominio público radioeléctrico para las redes y servicios de comunicaciones electrónicas;

u) contribuir a la protección de los derechos del usuario final en el sector de las comunicaciones electrónicas, en coordinación, en su caso, con otras autoridades competentes;

v) evaluar y supervisar las cuestiones de configuración del mercado y de competencia en relación con el acceso abierto a internet;

w) verificar el cumplimiento de los requisitos y las condiciones establecidas en el Reglamento (UE) 531/2012 del Parlamento Europeo y del Consejo, de 13 de junio de 2012, relativo a la itinerancia en las redes públicas de comunicaciones móviles en la Unión, en materia de acceso mayorista a los servicios de comunicaciones electrónicas de voz, SMS y datos en itinerancia en la Unión Europea, de sostenibilidad de la supresión de los recargos por itinerancia, de la correcta aplicación de las tarifas al por mayor de servicios regulados de itinerancia, de la publicación de la información actualizada relativa a la aplicación del citado Reglamento y de la resolución de conflictos entre operadores;

x) ser consultada por el Gobierno y el Ministerio de Asuntos Económicos y Transformación Digital en materia de comunicaciones electrónicas, particularmente en aquellas materias que puedan afectar al desarrollo libre y competitivo del mercado. Igualmente podrá ser consultada en materia de comunicaciones electrónicas por las Comunidades Autónomas y las Corporaciones Locales.

En el ejercicio de esta función, participará, mediante informe, en el proceso de elaboración de normas que afecten a su ámbito de competencias en materia de comunicaciones electrónicas;

y) realizar las funciones de arbitraje, tanto de derecho como de equidad, que le sean sometidas por los operadores de comunicaciones electrónicas en aplicación de la Ley 60/2003, de 23 de diciembre, de Arbitraje;

z) realizar las funciones atribuidas de manera expresa por la normativa europea, la presente ley y su normativa de desarrollo;

aa) realizar cualesquiera otras funciones que le sean atribuidas por ley o por real decreto;

ab) gestionar el Registro de operadores, conforme a lo establecido en el artículo 7;

ac) llevar a cabo la asignación de los derechos de uso de los recursos públicos regulados en los planes nacionales de numeración en los términos indicados en el capítulo VII del título II;

ad) gestionar en período voluntario las tasas en materia de telecomunicaciones a que se refiere la presente ley que no correspondan al Ministerio de Asuntos Económicos y Transformación Digital;

ae) velar por la sostenibilidad del modelo nacional de tarificación del operador y supervisar la evolución del mercado y de los precios de las comunicaciones intracomunitarias reguladas en los términos establecidos en el Reglamento (UE) 2015/2120 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015.

TÍTULO VII

Tasas en materia de telecomunicaciones

Artículo 101. *Tasas en materia de telecomunicaciones.*

1. Las tasas en materia de telecomunicaciones gestionadas por la Administración General del Estado serán las recogidas en el anexo I.
2. Dichas tasas tendrán como finalidad cubrir:

a) los gastos administrativos que ocasione el trabajo de regulación relativo a la preparación y puesta en práctica del derecho comunitario derivado y actos administrativos, como las relativas a la interconexión y acceso;
b) los gastos que ocasionen la gestión, control y ejecución del régimen establecido en esta ley;
c) los gastos que ocasionen la gestión, control y ejecución de los derechos de ocupación del dominio público, los derechos de uso del dominio público radioeléctrico y la numeración;
d) los gastos que ocasione la gestión de las notificaciones reguladas en el artículo 6.2;
e) los gastos de cooperación internacional, armonización y normalización y el análisis de mercado.

3. Sin perjuicio de lo dispuesto en el apartado 2, las tasas establecidas por reserva del dominio público radioeléctrico, la numeración y el dominio público necesario para la instalación de redes de comunicaciones electrónicas tendrán como finalidad la necesidad de garantizar el uso óptimo de estos recursos, teniendo en cuenta el valor del bien cuyo uso se otorga y su escasez. Dichas tasas deberán ser no discriminatorias, transparentes, justificadas objetivamente y ser proporcionadas a su fin. Asimismo, deberán fomentar el cumplimiento de los objetivos y principios establecidos en el artículo 3, en los términos que se establezcan mediante real decreto.
4. Las tasas a que se refieren los apartados anteriores serán impuestas de manera objetiva, transparente y proporcional, de manera que se minimicen los costes administrativos adicionales y las cargas que se derivan de ellos.
5. La instalación de los puntos de acceso inalámbrico para pequeñas áreas no está sujeta a la exigencia de tributos por ninguna Administración Pública, excepto la tasa general de operadores.
6. La revisión en vía administrativa de los actos de aplicación, gestión y recaudación de las tasas en materia de telecomunicaciones habrá de sujetarse a lo previsto en la Ley 58/2003, de 17 de diciembre, General Tributaria y su normativa de desarrollo.
7. La Comisión Nacional de los Mercados y la Competencia respecto de las tasas a las que se refiere el apartado 1, y las Administraciones competentes que gestionen y liquiden tasas subsumibles en el apartado 2 de este artículo, publicarán un resumen anual de los gastos administrativos que justifican su imposición y del importe total de la recaudación. Asimismo, las Administraciones competentes que gestionen y liquiden tasas subsumibles en el apartado 3 de este artículo publicarán anualmente el importe total de la recaudación obtenida de los operadores de redes y servicios de comunicaciones electrónicas.

TÍTULO VIII

Inspección y régimen sancionador

Artículo 102. *Funciones inspectoras.*

1. La función inspectora en materia de telecomunicaciones corresponde a:

a) el Ministerio de Asuntos Económicos y Transformación Digital;
b) la Comisión Nacional de los Mercados y la Competencia.

2. Será competencia del Ministerio de Asuntos Económicos y Transformación Digital la inspección de aquellas actuaciones sobre las que tenga atribuida competencia sancionadora de conformidad con esta ley y su normativa de desarrollo y, en particular, la inspección:

a) de los servicios y de las redes de comunicaciones electrónicas y de sus condiciones de prestación y explotación;

b) de las obligaciones de servicio público y derechos y obligaciones de carácter público en la instalación y explotación de redes y en la prestación de servicios de comunicaciones electrónicas;

c) de los equipos de telecomunicación, de las instalaciones y de los sistemas civiles;

d) del dominio público radioeléctrico;

e) de las tasas en materia de telecomunicaciones;

f) de los servicios de tarificación adicional que se soporten sobre redes y servicios de comunicaciones electrónicas.

3. Corresponderá a la Comisión Nacional de los Mercados y la Competencia, en los términos establecidos en la Ley 3/2013, de 4 de junio, de creación de la Comisión Nacional de los Mercados y la Competencia, la inspección de las actividades de los operadores de comunicaciones electrónicas respecto de las cuales tenga competencia sancionadora de conformidad con esta ley y su normativa de desarrollo.

4. Para la realización de determinadas actividades de inspección técnica, la Comisión Nacional de los Mercados y la Competencia, en materias de su competencia en el ámbito de aplicación de esta ley, podrá solicitar la actuación del Ministerio de Asuntos Económicos y Transformación Digital.

Artículo 103. *Facultades de inspección.*

1. Los funcionarios destinados en la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales del Ministerio de Asuntos Económicos y Transformación Digital que tengan asignadas funciones de inspección, ya sea en servicios centrales o periféricos, y el personal funcionario de carrera de la Comisión Nacional de los Mercados y la Competencia específicamente designado para ello tienen, en el ejercicio de sus funciones inspectoras en materia de telecomunicaciones, la consideración de autoridad pública y podrán solicitar, a través de la autoridad gubernativa correspondiente, el apoyo necesario de los Cuerpos y Fuerzas de Seguridad.

2. Los operadores o quienes realicen las actividades a las que se refiere esta ley vendrán obligados a facilitar al personal que tenga asignadas funciones de inspección, en el ejercicio de sus funciones, el acceso a sus instalaciones. También deberán permitir que dicho personal lleve a cabo el control de los elementos afectos a los servicios o actividades que realicen, de las redes que suministren y de cuantos documentos están obligados a poseer o conservar.

Los titulares de fincas o bienes inmuebles en los que se ubiquen equipos, estaciones o cualquier clase de instalaciones de telecomunicaciones tendrán la obligación de permitir el acceso a dichos bienes por parte del personal de inspección a que se refiere este artículo. A estos efectos, el acceso por el personal de inspección a las mencionadas fincas o inmuebles requerirá el consentimiento de dichos titulares o autorización judicial solo cuando sea necesario entrar en un domicilio constitucionalmente protegido o efectuar registros en el mismo. Los órganos jurisdiccionales de lo contencioso-administrativo resolverán sobre el otorgamiento de la autorización judicial en el plazo máximo de setenta y dos horas.

Igualmente, los operadores y titulares mencionados deberán facilitar al personal que tenga asignadas funciones de inspección la realización de las pruebas técnicas o actuaciones complementarias dirigidas a dilucidar el origen o las consecuencias de las presuntas actuaciones infractoras que dicho personal de inspección les requiera, ya sean dentro o fuera de las instalaciones.

3. Los operadores o quienes realicen las actividades a las que se refiere esta ley quedan obligados a poner a disposición del personal de inspección cuantos libros, registros y documentos, sea cual fuere su forma y soporte, y medios técnicos este considere precisos, incluidos el software, los programas informáticos y los archivos magnéticos, ópticos o de cualquier otra clase, pudiendo al efecto el personal de inspección hacer u obtener copias de ellos.

Asimismo, deberán facilitarles, a su petición, cualquier tipo de documentación que el personal de la inspección les exija para la determinación de la titularidad de los equipos o la

autoría de emisiones, actividades o de los contenidos o servicios que se presten a través de las redes de comunicaciones electrónicas.

4. Las obligaciones establecidas en los dos apartados anteriores serán exigibles a los operadores o quienes realicen las actividades a las que se refiere esta ley y su normativa de desarrollo y que sean directamente responsables del suministro de la red, la prestación del servicio o la realización de la actividad regulada por esta ley, y también serán exigibles a quienes den soporte a las actuaciones anteriores, a los titulares de las fincas o los inmuebles en donde se ubiquen equipos o instalaciones de telecomunicaciones, a las asociaciones de empresas y a los administradores y otros miembros del personal de todas ellas.

5. Los operadores o quienes realicen las actividades a las que se refiere esta ley y su normativa de desarrollo están obligados a someterse a las inspecciones que efectúe el personal de inspección. La negativa u obstrucción al acceso a las instalaciones, fincas o bienes inmuebles, a comparecer a los actos de inspección a los cuales haya sido citados, a la realización de las pruebas técnicas o actuaciones complementarias requeridas o a facilitar la información o documentación requerida será sancionada, conforme a los artículos siguientes de este título, como obstrucción a la labor inspectora.

6. En particular, el personal de inspección tendrá las siguientes facultades:

a) precintar todos los locales, instalaciones, equipos, libros o documentos y demás bienes de la empresa durante el tiempo y en la medida en que sea necesario para la inspección;

b) realizar comprobaciones, mediciones, obtener fotografías, vídeos, y grabaciones de imagen o sonido.

7. Las actuaciones de inspección, comprobación o investigación llevadas a cabo por el personal de inspección podrán desarrollarse, a su elección:

a) en cualquier despacho, oficina o dependencia de la persona o entidad inspeccionada o de quien las represente;

b) en los propios locales de la autoridad de inspección;

c) en cualquier despacho, oficina, dependencia o lugar en los que existan pruebas de los hechos objeto de inspección.

8. El personal de inspección, a los efectos del cumplimiento de las funciones previstas en este artículo, tendrá acceso gratuito a todo registro público, en particular, en los Registros de la Propiedad y Mercantiles. El acceso a la información registral se realizará por medios electrónicos, en la forma determinada en su normativa reguladora.

9. El personal de inspección, en el ejercicio de sus funciones de control y supervisión del adecuado uso del dominio público radioeléctrico, podrá colaborar con el de otros Estados. En particular, el personal de inspección deberá tramitar las solicitudes que se presenten y remitir la documentación oportuna a los órganos competentes en los supuestos de emisiones de estaciones radioeléctricas ubicadas en territorio español que produzcan interferencias en las redes y servicios de otros Estados. En estos supuestos, los documentos procedentes de las autoridades competentes de otros Estados, emitidos conforme a los tratados internacionales de que España sea parte acreditarán la producción de las interferencias.

Artículo 104. *Responsabilidad por las infracciones en materia de telecomunicaciones.*

La responsabilidad administrativa por las infracciones de las normas reguladoras de las telecomunicaciones será exigible:

a) en el caso de incumplimiento de las condiciones establecidas para la instalación o explotación de redes o la prestación de servicios de comunicaciones electrónicas, a la persona física o jurídica que desarrolle la actividad;

b) en las cometidas con motivo del suministro de redes o la prestación de servicios de comunicaciones electrónicas sin haber efectuado la notificación a que se refiere el artículo 6.2 o sin disponer de título habilitante para el uso del dominio público radioeléctrico cuando dicho título sea necesario, a la persona física o jurídica que realice la actividad.

Para identificar a la persona física o jurídica que realiza la actividad, se puede solicitar colaboración a la persona física o jurídica que tenga la disponibilidad de los equipos e instalaciones por cualquier título jurídico válido en derecho o careciendo de éste o a la

persona física o jurídica titular de la finca o inmueble en donde se ubican los equipos e instalaciones. Si, practicada la notificación del requerimiento de colaboración conforme a lo establecido en la Ley 39/2015, de 1 de octubre, no se presta la citada colaboración, se considerará que la misma es responsable de las infracciones cometidas por quien realiza la actividad. Esta responsabilidad es solidaria de la exigible a la persona física o jurídica que realiza la actividad;

c) en las cometidas por los usuarios, por las empresas instaladoras de telecomunicación, por los operadores económicos relacionados con equipos de telecomunicación o por otras personas que, sin estar comprendidas en los párrafos anteriores, realicen actividades reguladas en la normativa sobre telecomunicaciones, a la persona física o jurídica cuya actuación se halle tipificada por el precepto infringido o a la que las normas correspondientes atribuyen específicamente la responsabilidad;

d) en el caso de infracciones cometidas en materia de evaluación de la conformidad y puesta en el mercado de equipos de telecomunicación, será compatible la exigencia de responsabilidad de distintos agentes por los mismos hechos, en función de las obligaciones establecidas a cada uno de ellos por la legislación de armonización de la Unión Europea en materia de equipos de telecomunicación, esta ley y su normativa de desarrollo.

Artículo 105. *Clasificación de las infracciones.*

Las infracciones de las normas reguladoras de las telecomunicaciones se clasifican en muy graves, graves y leves.

Artículo 106. *Infracciones muy graves.*

Se consideran infracciones muy graves:

1. La realización de actividades sin disponer de la habilitación oportuna en las materias reguladas por esta ley, cuando legalmente sea necesaria.

2. El incumplimiento de los requisitos exigibles para el suministro de las redes y prestación de los servicios de comunicaciones electrónicas establecidos en el artículo 6.1.

3. El incumplimiento de la obligación de notificación al Registro de operadores establecida en los artículos 6.2.

4. La utilización del dominio público radioeléctrico, frecuencias o canales radioeléctricos sin disponer de la concesión de uso privativo del dominio público radioeléctrico a que se refiere el artículo 88, cuando legalmente sea necesario.

5. La utilización del dominio público radioeléctrico, frecuencias o canales radioeléctricos no adecuada al correspondiente plan de utilización del espectro radioeléctrico o al Cuadro Nacional de Atribución de Frecuencias.

6. La realización de emisiones radioeléctricas no autorizadas que vulneren o perjudiquen el desarrollo o implantación de lo establecido en los planes de utilización del dominio público radioeléctrico o en el Cuadro Nacional de Atribución de Frecuencias.

7. La producción deliberada, en España o en los países vecinos, de interferencias a redes o servicios autorizados, incluidas las causadas por estaciones radioeléctricas que estén instaladas o en funcionamiento a bordo de un buque, de una aeronave o de cualquier otro objeto flotante o aerotransportado que transmita emisiones desde fuera del territorio español para su posible recepción total o parcial en este.

8. No atender el requerimiento de cesación formulado por la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, en los supuestos de producción de interferencias.

9. La importación, comercialización, publicidad, cesión de forma gratuita u onerosa, instalación, tenencia, puesta en servicio o uso de cualquier equipo con funcionalidades para la generación intencionada de interferencias a equipos, redes o servicios de telecomunicaciones, salvo cuando estas actividades estén amparadas por la excepción prevista en el artículo 82.4.

10. El incumplimiento grave de las obligaciones en materia de interconexión e interoperabilidad de los servicios, incluyendo los compromisos convertidos en vinculantes para los operadores relativos a las condiciones de acceso o de coinversión.

11. El incumplimiento grave de las características y condiciones establecidas para la conservación de los números.

12. El incumplimiento por los operadores y otros agentes que intervienen en el mercado de las telecomunicaciones de las resoluciones firmes en vía administrativa dictadas en las controversias a que se refiere el artículo 78.

13. El incumplimiento de las resoluciones firmes en vía administrativa o de las medidas previas al procedimiento sancionador o de las medidas cautelares acordadas dentro de éste a que se refieren los artículos 111 y 112 dictadas por el Ministerio de Asuntos Económicos y Transformación Digital en el ejercicio de sus funciones atribuidas por esta ley.

14. El incumplimiento de las resoluciones firmes en vía administrativa o de las medidas cautelares a que se refieren los artículos 111 y 112 dictadas por la Comisión Nacional de los Mercados y la Competencia en el ejercicio de sus funciones en materia de comunicaciones electrónicas, con excepción de las que se lleven a cabo en el procedimiento arbitral previo sometimiento voluntario de las partes.

15. La interceptación, sin autorización, de telecomunicaciones no destinadas al público en general, así como la divulgación del contenido.

16. El incumplimiento reiterado mediante infracciones tipificadas como graves en los términos expresados en el artículo 109.6.

Artículo 107. *Infracciones graves.*

Se consideran infracciones graves:

1. La instalación de estaciones radioeléctricas sin autorización, cuando, de acuerdo con lo dispuesto en la normativa reguladora de las telecomunicaciones, sea necesaria.

2. La instalación de estaciones radioeléctricas con características distintas a las autorizadas o, en su caso, a las contenidas en el proyecto técnico aprobado, incluyendo las estaciones radioeléctricas a bordo de un buque, de una aeronave o de cualquier otro objeto flotante o aerotransportado, que, en el mar o fuera de él, posibilite la transmisión de emisiones desde el exterior para su posible recepción total o parcial en territorio nacional.

3. El uso del dominio público radioeléctrico en condiciones distintas a las previstas en la concesión para el uso privativo del dominio público radioeléctrico a que se refiere el artículo 88, o, en su caso, distintas de las aprobadas en el proyecto técnico de las instalaciones, entre ellas utilizando parámetros técnicos distintos de los propios de la concesión o potencias de emisión superiores a las autorizadas.

4. El emplazamiento de estaciones radioeléctricas en ubicaciones diferentes de las aprobadas.

5. La utilización del dominio público radioeléctrico, frecuencias o canales radioeléctricos sin disponer de la autorización general, autorización individual o afectación demanial para el uso privativo del dominio público radioeléctrico, cuando legalmente sea necesario.

6. La mera producción, en España o en los países vecinos, de interferencias a redes o servicios autorizados que no se encuentren comprendidas en el artículo anterior.

7. Efectuar emisiones radioeléctricas que incumplan los límites de exposición establecidos en la normativa de desarrollo del artículo 86 o incumplir las demás medidas de seguridad establecidas en ella, incluidas las obligaciones de señalización o vallado de las instalaciones radioeléctricas. Asimismo, contribuir, mediante emisiones no autorizadas, a que se incumplan dichos límites.

8. La realización de operaciones de mercado secundario de títulos habilitantes o derechos de uso del dominio público radioeléctrico, sin cumplir con los requisitos establecidos a tal efecto por la normativa de desarrollo de esta ley.

9. La puesta a disposición de redes públicas de comunicaciones electrónicas o de cualquier elemento de red que contribuya a la transmisión de la señal a favor de entidades para que se realicen emisiones radioeléctricas cuando no se ostente el correspondiente título habilitante para el uso del dominio público radioeléctrico.

10. La presentación de declaraciones responsables sustitutivas de aprobación de proyectos técnicos de radiocomunicaciones, de certificaciones sustitutivas de la inspección previa de instalaciones radioeléctricas o de certificaciones de cumplimiento de los niveles de emisión radioeléctrica tolerable que no concuerden con la realidad o relativas a estaciones

radioeléctricas respecto de las cuales, con posterioridad, se constaten incumplimientos de la normativa de telecomunicaciones que hubieran debido ser detectados en ellas.

11. El incumplimiento de las obligaciones que se deriven de las designaciones o acreditaciones que realice la Administración de telecomunicaciones en materia de evaluación de la conformidad de equipos de telecomunicación, de conformidad con la normativa europea y nacional que les sean de aplicación.

12. La importación o comercialización de equipos de telecomunicación cuya conformidad con los requisitos esenciales aplicables no haya sido evaluada de acuerdo con lo dispuesto en el título IV y su normativa de desarrollo, o con las disposiciones, los acuerdos o convenios internacionales que obliguen al Estado español.

13. La instalación, puesta en servicio o utilización de equipos de telecomunicación cuya conformidad con los requisitos esenciales aplicables no haya sido evaluada de acuerdo con lo dispuesto en el título IV y su normativa de desarrollo.

14. El ejercicio de la actividad de instalación y mantenimiento de equipos y sistemas de telecomunicación sin haber efectuado la declaración responsable o sin cumplir los requisitos a los que se refiere el artículo 84.

15. La instalación de infraestructuras comunes de telecomunicación en el interior de edificios y conjuntos inmobiliarios que sean causa de daños en las redes públicas de comunicaciones electrónicas.

16. La alteración, la manipulación o la omisión de las características técnicas en la documentación de las instalaciones comunes de telecomunicación en el interior de edificios y conjuntos inmobiliarios que se presente a la Administración o a los propietarios.

17. El incumplimiento de las condiciones para el suministro de redes o la prestación de servicios de comunicaciones electrónicas establecidas en esta ley y su normativa de desarrollo.

18. El incumplimiento por los operadores controlados directa o indirectamente por Administraciones públicas de las obligaciones establecidas en el artículo 13.

19. El incumplimiento de las condiciones establecidas en los planes nacionales de numeración o sus disposiciones de desarrollo o en las atribuciones y asignaciones de los derechos de uso de los recursos de numeración incluidos en los planes de numeración.

20. El incumplimiento de las condiciones asociadas al uso de numeración atribuida a los servicios de tarificación adicional.

21. El incumplimiento de las obligaciones relacionadas con la utilización de normas o especificaciones técnicas declaradas obligatorias por la Comisión Europea.

22. El incumplimiento de las obligaciones relativas a la integridad y seguridad en la prestación de servicios o el suministro de redes de comunicaciones electrónicas.

23. El incumplimiento de las obligaciones establecidas para la utilización compartida del dominio público o la propiedad privada en que se van a establecer las redes públicas de comunicaciones electrónicas o el uso compartido de las infraestructuras y recursos asociados.

24. El incumplimiento de las obligaciones establecidas para la utilización compartida de los tramos finales de las redes de acceso.

25. El incumplimiento de las obligaciones en materia de acceso a redes, de acceso a infraestructuras físicas susceptibles de alojar redes públicas de comunicaciones electrónicas y obras civiles y su coordinación, de las obligaciones de transparencia o información mínima respecto de las mismas, así como en materia de interconexión e interoperabilidad de los servicios, incluyendo los compromisos convertidos en vinculantes para los operadores relativos a las condiciones de acceso o de coinversión.

26. Cursar tráfico no permitido o tráfico irregular con fines fraudulentos en las redes públicas y servicios de comunicaciones electrónicas disponibles al público.

27. El incumplimiento de las características y condiciones establecidas para el cambio de operador y la conservación de los números, así como para el cambio de proveedor de los servicios de acceso a internet.

28. El incumplimiento de la normativa en materia de itinerancia en la Unión Europea e internacional.

29. El incumplimiento de las obligaciones de servicio público según lo establecido en el título III y su normativa de desarrollo.

30. La vulneración de los derechos de los consumidores y usuarios finales, según lo establecido en el título III y su normativa de desarrollo, incluidos los derechos de conservación de número, de itinerancia en la Unión Europea e internacional, en materia de comunicaciones intracomunitarias reguladas y acceso abierto a internet.

31. El cumplimiento tardío o defectuoso por los operadores y otros agentes que intervienen en el mercado de las telecomunicaciones de las resoluciones firmes en vía administrativa dictadas en las controversias a que se refieren el artículo 78.

32. Proporcionar información engañosa, errónea o incompleta a sabiendas o con negligencia grave para la elaboración de los estudios geográficos a que se refiere el artículo 48.

33. El incumplimiento, por causas imputables al operador, del compromiso en firme de desplegar, extender o mejorar redes de banda ancha en los términos indicados en el artículo 48, que produzca un perjuicio al interés público en el diseño de planes nacionales de banda ancha, en la determinación de obligaciones de cobertura ligadas a los derechos de uso del espectro radioeléctrico o en la verificación de la disponibilidad de servicios en el marco de la obligación de servicio universal, o bien un perjuicio a otro operador.

34. No facilitar, cuando resulte exigible conforme a lo previsto por la normativa reguladora de las comunicaciones electrónicas, los datos requeridos por la Administración de telecomunicaciones una vez transcurridos un mes a contar desde la finalización del plazo otorgado en el requerimiento de información o una vez finalizado el plazo otorgado en el segundo requerimiento de la misma información, así como aportar información inexacta o falsa en cualquier dato, manifestación o documento que se presente a la Administración de telecomunicaciones.

35. La falta de notificación a la Administración por el titular de una red de comunicaciones electrónicas de los servicios que se estén prestando a través de ella cuando esta información sea exigible de acuerdo con la normativa aplicable.

36. La negativa o la obstrucción a ser inspeccionado, la no colaboración con la inspección cuando esta sea requerida y la no identificación por la persona física o jurídica que tenga la disponibilidad de los equipos e instalaciones o sea titular de la finca o inmueble en donde se ubican los equipos e instalaciones de la persona física o jurídica que suministre redes o preste servicios.

37. El cumplimiento tardío o defectuoso de las resoluciones firmes en vía administrativa o de las medidas previas y medidas cautelares a que se refieren los artículos 111 y 112 dictadas por el Ministerio de Asuntos Económicos y Transformación Digital en el ejercicio de sus funciones en materia de comunicaciones electrónicas.

38. El cumplimiento tardío o defectuoso de las resoluciones firmes en vía administrativa o de las medidas previas y medidas cautelares a que se refieren los artículos 111 y 112 dictadas por la Comisión Nacional de los Mercados y la Competencia en el ejercicio de sus funciones en materia de comunicaciones electrónicas, con excepción de las que se lleve a cabo en el procedimiento arbitral previo sometimiento voluntario de las partes.

39. El incumplimiento grave de las obligaciones en materia de calidad de servicio establecidas en esta ley y su normativa de desarrollo,

40. El incumplimiento de las obligaciones establecidas en el artículo 76 y su normativa de desarrollo, así como en el Reglamento (UE) 2015/2120 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015.

41. El incumplimiento de la normativa en materia de comunicaciones intracomunitarias reguladas.

42. El incumplimiento por los titulares de las infraestructuras físicas desde las que los operadores efectúen materialmente emisiones radioeléctricas mediante el uso del dominio público radioeléctrico de tener identificada la titularidad de cada uno de los transmisores instalados susceptibles de producir emisiones radioeléctricas o de tener una relación actualizada de las frecuencias utilizadas por cada transmisor.

43. El incumplimiento de las obligaciones en materia de interceptación legal de comunicaciones impuestas en desarrollo del artículo 58.

44. El incumplimiento reiterado mediante infracciones tipificadas como leves en los términos expresados en el artículo 109.6.

Artículo 108. *Infracciones leves.*

Se consideran infracciones leves:

1. La producción de cualquier tipo de emisión radioeléctrica no autorizada, salvo que deba ser considerada como infracción grave o muy grave.
2. El establecimiento de comunicaciones utilizando estaciones no autorizadas, salvo que deba ser considerada como infracción grave.
3. La utilización del dominio público radioeléctrico, frecuencias o canales radioeléctricos sin disponer de la autorización para el uso especial del dominio público radioeléctrico, cuando legalmente sea necesario.
4. La instalación de estaciones radioeléctricas de radioaficionado careciendo de autorización.
5. El incumplimiento por los titulares de autorizaciones generales, autorizaciones individuales o afectaciones demaniales para el uso del dominio público radioeléctrico de las condiciones autorizadas o que se les impongan por el Ministerio de Asuntos Económicos y Transformación Digital.
6. El suministro de redes o la prestación de servicios de comunicaciones electrónicas sin cumplir los requisitos exigibles para realizar tales actividades establecidos en esta ley y su normativa de desarrollo, distintos de los previstos en los artículos 6.1 y 6.2.
7. El incumplimiento de las obligaciones que tiene el fabricante, el representante autorizado de un fabricante, el importador, el prestador de servicios logísticos o el distribuidor de equipos de telecomunicación, según lo dispuesto en el título IV y su normativa de desarrollo, salvo que deba ser considerado como infracción grave o muy grave.
8. El incumplimiento de las obligaciones relacionadas con la puesta en servicio y utilización de equipos de telecomunicación, según lo dispuesto en el título IV y su normativa de desarrollo, salvo que deba ser considerado como infracción grave o muy grave.
9. La no presentación de la documentación de las instalaciones comunes de telecomunicaciones a la administración o a la propiedad, cuando normativamente sea obligatoria dicha presentación, o el incumplimiento de los requisitos en la presentación de la documentación o en la ejecución de las instalaciones comunes de telecomunicaciones.
10. La instalación de infraestructuras de telecomunicaciones sin cumplir los requisitos establecidos en la presente ley, salvo que deba ser considerada como infracción grave o muy grave.
11. El incumplimiento de las obligaciones de carácter público, según lo establecido en el título III y su normativa de desarrollo.
12. No facilitar los datos requeridos por la Administración de telecomunicaciones o retrasar injustificadamente su aportación cuando resulte exigible conforme a lo previsto por la normativa reguladora de las comunicaciones electrónicas.
13. La expedición de declaraciones responsables sustitutivas de aprobación de proyectos técnicos de radiocomunicaciones, de certificaciones sustitutivas de la inspección previa de instalaciones radioeléctricas o de certificaciones de cumplimiento de los niveles de emisión radioeléctrica tolerable que no concuerden con la realidad o relativas a estaciones radioeléctricas respecto de las cuales, con posterioridad, se constaten incumplimientos de la normativa de telecomunicaciones que hubieran debido ser detectados en ellas.

Artículo 109. *Sanciones.*

1. Por la comisión de las infracciones tipificadas en los artículos anteriores se impondrán las siguientes sanciones:

a) por la comisión de infracciones muy graves se impondrá al infractor multa por importe de hasta veinte millones de euros.

Por la comisión de infracciones muy graves tipificadas en las que la Comisión Nacional de los Mercados y la Competencia tenga competencias sancionadoras se impondrá al infractor multa por importe no inferior al tanto, ni superior al quíntuplo, del beneficio bruto obtenido como consecuencia de los actos u omisiones en que consista la infracción. En caso de que no resulte posible aplicar este criterio, el límite máximo de la sanción será el dos por ciento del volumen de negocios total obtenido por la entidad infractora en el último ejercicio;

b) las infracciones muy graves, en función de sus circunstancias, podrán dar lugar a la inhabilitación hasta de cinco años del operador para el suministro de redes o la prestación de servicios de comunicaciones electrónicas. También podrá dar lugar a la inhabilitación hasta cinco años para el ejercicio de la actividad de instalador;

c) por la comisión de infracciones graves se impondrá al infractor multa por importe de hasta dos millones de euros.

Por la comisión de infracciones graves tipificadas en las que la Comisión Nacional de los Mercados y la Competencia tenga competencias sancionadoras se impondrá al infractor multa por importe de hasta el duplo del beneficio bruto obtenido como consecuencia de los actos u omisiones que constituyan aquellas o, en caso de que no resulte aplicable este criterio, el límite máximo de la sanción será el uno por ciento del volumen de negocios total obtenido por la entidad infractora en el último ejercicio;

d) por la comisión de infracciones leves se impondrá al infractor una multa por importe de hasta 100.000 euros.

2. Las sanciones impuestas por cualquiera de las infracciones comprendidas en los artículos 106, 107 y 108 podrán llevar aparejada, como sanción accesoria, en tanto no se disponga del título habilitante que resulte necesario para el ejercicio de la actividad realizada por el infractor, o teniendo dicho título, mientras se efectúen emisiones radioeléctricas con parámetros o características técnicas distintas a las autorizadas:

a) el cese inmediato de emisiones radioeléctricas no autorizadas, ya sea por carecer de título habilitante o por efectuarse con parámetros o características técnicas distintas a las autorizadas;

b) el ajuste de las emisiones radioeléctricas a los parámetros y características técnicas autorizadas;

c) el precintado o la incautación de los equipos de telecomunicación;

d) la clausura de las instalaciones.

3. Las sanciones impuestas por cualquiera de las infracciones comprendidas en los artículos 106, 107 y 108 podrán llevar aparejada, en caso de equipos de telecomunicación que no cumplan los requisitos para su comercialización, la retirada o recuperación del mercado de los mismos o la prohibición o restricción de su comercialización, hasta que se produzca el cumplimiento de dichos requisitos.

4. Las sanciones impuestas por vulneración de las condiciones establecidas para la utilización de la numeración podrán llevar aparejada orden de imposibilidad de uso del número o números a través de los cuales se ha producido el incumplimiento, por un período máximo de dos años.

5. Además de la sanción que corresponda imponer a los infractores, cuando se trate de una persona jurídica, se podrá imponer una multa de hasta 5.000 euros en el caso de las infracciones leves, hasta 30.000 euros en el caso de las infracciones graves y hasta 60.000 euros en el caso de las infracciones muy graves a sus representantes legales o a las personas que integran los órganos directivos o los órganos colegiados de administración que hayan intervenido en el acuerdo o decisión.

Quedan excluidas de la sanción aquellas personas que, formando parte de órganos directivos o de los órganos colegiados de administración, no hubieran asistido a las reuniones o hubieran votado en contra o salvando su voto.

6. A los efectos de lo establecido en esta ley, tendrá la consideración de incumplimiento reiterado la sanción firme en vía administrativa por la comisión de dos o más infracciones del mismo tipo infractor en un período de tres años.

Artículo 110. *Criterios para la determinación de la cuantía de la sanción.*

1. La cuantía de la sanción que se imponga, dentro de los límites indicados, se graduará teniendo en cuenta, además de lo previsto en el artículo 29 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, lo siguiente:

a) la gravedad de las infracciones cometidas anteriormente por el sujeto al que se sanciona;

b) el daño causado, como la producción de interferencias a terceros autorizados, y su reparación;

c) el cumplimiento voluntario de las medidas cautelares que, en su caso, se impongan en el procedimiento sancionador;

d) la negativa u obstrucción al acceso a las instalaciones o a facilitar la información o documentación requerida;

e) el cese de la actividad infractora, previamente o durante la tramitación del expediente sancionador;

f) la afectación a bienes jurídicos protegidos relativos al uso del dominio público radioeléctrico, el orden público, la seguridad pública y la seguridad nacional o los derechos de los usuarios;

g) la colaboración activa y efectiva con la autoridad competente en la detección o prueba de la actividad infractora.

2. En el caso de la infracción consistente en proporcionar información engañosa, errónea o incompleta a sabiendas o con negligencia grave para la elaboración de los estudios geográficos a que se refiere el artículo 48 tipificada en el artículo 107.32, en la fijación de la cuantía de la sanción se tendrá en cuenta, entre otros criterios, si el comportamiento de la empresa o autoridad pública ha tenido un efecto negativo sobre la competencia y, en particular, si, contrariamente a la información proporcionada originalmente o a cualquier actualización de la misma, la empresa o autoridad pública ha desplegado, extendido o mejorado una red o no ha desplegado una red y ha incumplido su obligación de presentar una justificación objetiva para este cambio de planes.

3. El infractor vendrá obligado, en su caso, al pago de las tasas que hubiera debido satisfacer en el supuesto de haber realizado la notificación a que se refiere el artículo 6.2 o de haber disfrutado de título para la utilización del dominio público radioeléctrico.

Artículo 111. *Medidas previas al procedimiento sancionador.*

1. Previamente al inicio del procedimiento sancionador, podrá ordenarse por el órgano competente del Ministerio de Asuntos Económicos y Transformación Digital o de la Comisión Nacional de los Mercados y la Competencia, mediante resolución motivada sin audiencia previa, el cese de la presunta actividad infractora cuando existan razones de imperiosa urgencia basada en alguno de los siguientes supuestos:

a) cuando exista una amenaza inmediata y grave para el orden público, la seguridad pública o la seguridad nacional;

b) cuando exista una amenaza inmediata y grave para la salud pública;

c) cuando de la supuesta actividad infractora puedan producirse perjuicios graves al funcionamiento de los servicios de seguridad pública, protección civil y de emergencias;

d) cuando se interfiera gravemente a otros servicios o redes de comunicaciones electrónicas;

e) cuando cree graves problemas económicos u operativos a otros proveedores o usuarios de redes o servicios de comunicaciones electrónicas o demás usuarios del dominio público radioeléctrico.

2. Esta orden de cese irá dirigida a cualquier sujeto que se encuentre en disposición de ejecutar tal cese, sin perjuicio de la posterior delimitación de responsabilidades en el correspondiente procedimiento sancionador. Para su ejecución forzosa, la resolución podrá disponer que, a través de la autoridad gubernativa, se facilite apoyo por los Cuerpos y Fuerzas de Seguridad.

3. En la resolución se determinará el ámbito objetivo y temporal de la medida, sin que pueda exceder del plazo de quince días hábiles.

La resolución a la que se refiere este apartado será directamente recurrible ante el orden jurisdiccional contencioso-administrativo.

4. En los supuestos en los que la imposición de la medida previa y excepcional de cese de actividad pudiera afectar a una señal radioeléctrica, redes de comunicaciones electrónicas o sitio web, tal medida deberá en todo caso ser conocida por los usuarios de dichos servicios afectados debiendo quedar reflejado al acceder a la señal radioeléctrica mediante imagen visualizada o anuncio sonoro, o al acceder al sitio web, en el que se

informe que el mismo ha sido bloqueado y la información relevante sobre dicha circunstancia, información que deberá incluir la base legal para el bloqueo, la fecha y el número de la decisión de bloqueo, el organismo emisor, así como el texto de la decisión de bloqueo, incluyendo las razones de la misma, y las vías de recurso, debiendo quedar reflejada esta información por espacio temporal de un mes.

5. En el plazo de quince días hábiles siguientes a su adopción y previa audiencia del interesado para que pueda proponer soluciones debe confirmarse, modificarse o levantarse la orden de cese, lo que se efectuará en el acuerdo de iniciación del procedimiento sancionador.

6. En todo caso, será de aplicación con carácter supletorio lo dispuesto en el artículo 56 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Artículo 112. *Medidas cautelares en el procedimiento sancionador.*

1. Una vez incoado el procedimiento sancionador, las infracciones a las que se refieren los artículos 106, 107 y 108, de conformidad con el artículo 56 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, podrán dar lugar a la adopción de las siguientes medidas cautelares:

a) ordenar el cese inmediato de emisiones radioeléctricas no autorizadas;

b) ordenar el cese inmediato de cualquier otra actividad presuntamente infractora. Entre ellas:

1.º poner fin a la prestación de un servicio o de una serie de servicios, o aplazarla cuando dicha prestación pudiera tener como resultado perjudicar seriamente la competencia, hasta que se cumplan las obligaciones específicas impuestas a raíz de un análisis de mercado con arreglo al artículo 18. Esta medida, junto con las razones en que se basa, se comunicará al operador afectado sin demora, fijando un plazo razonable para que la empresa cumpla con la misma;

2.º impedir que un operador siga suministrando redes o servicios de comunicaciones electrónicas o suspender o retirarle sus derechos de uso, en caso de incumplimiento grave y reiterado de las condiciones establecidas para la prestación de servicios o el suministro de redes o para el otorgamiento de derechos de uso o de las obligaciones específicas que se hubieran impuesto, cuando hubieran fracasado las medidas destinadas a exigir el cese de la infracción;

3.º confirmar o modificar las medidas provisionales de urgencia adoptadas conforme a lo dispuesto en el artículo anterior. Estas medidas provisionales serán válidas durante tres meses como máximo, prorrogables por otro período de hasta tres meses;

c) ordenar el ajuste y la adecuación de las emisiones a los parámetros y condiciones técnicas autorizadas;

d) ordenar el precintado de los equipos o instalaciones que hubiera empleado el infractor, siendo, en su caso, aplicable el régimen de ejecución subsidiaria previsto en el artículo 102 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas;

e) ordenar la retirada o su recuperación del mercado de los equipos de telecomunicación que presuntamente no hayan evaluado su conformidad de acuerdo con la normativa aplicable;

f) la suspensión provisional de la eficacia del título y la clausura provisional de las instalaciones, por un plazo máximo de seis meses.

2. Cuando el presunto infractor carezca de título habilitante para la ocupación o uso del dominio público radioeléctrico, vulnere o condicione la adecuada ejecución de los planes técnicos de uso del dominio público radioeléctrico, produzca interferencias a servicios legalmente autorizados o si con la infracción se superan los niveles de emisiones radioeléctricas establecidos en la normativa de desarrollo del artículo 86, la medida cautelar prevista en la letra a) y, en su caso, en la letra c) del apartado anterior será obligatoriamente incluida en el acuerdo de iniciación de expediente sancionador, con objeto de salvaguardar el correcto uso de dicho dominio público.

3. Sin perjuicio de los supuestos en los que este precepto fija un plazo máximo de duración, las medidas cautelares podrán mantenerse hasta la resolución del procedimiento sancionador, siempre que se considere necesario para asegurar la eficacia de la resolución final que pudiera recaer. Como excepción, la medida cautelar de retirada o su recuperación del mercado de los equipos de telecomunicación cuya conformidad no haya sido evaluada presuntamente de acuerdo con la normativa aplicable deberá levantarse cuando se acredite la realización de la evaluación de la conformidad de los equipos de telecomunicación afectados.

Artículo 113. *Prescripción.*

1. Las infracciones muy graves prescribirán a los tres años, las graves a los dos años y las leves al año.

El plazo de prescripción de las infracciones comenzará a computarse desde el día en que se hubieran cometido. Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador. El plazo de prescripción volverá a correr si el expediente sancionador estuviera paralizado durante más de un mes por causa no imputable al presunto responsable.

En el supuesto de infracción continuada, la fecha inicial del cómputo será aquella en que deje de realizarse la actividad infractora o la del último acto con que la infracción se consume. No obstante, se entenderá que persiste la infracción en tanto los equipos de telecomunicación o instalaciones objeto del expediente no se encuentren a disposición de la Administración o quede constancia fehaciente de su imposibilidad de uso.

2. Las sanciones impuestas por faltas muy graves prescribirán a los tres años; las impuestas por faltas graves, a los dos años, y las impuestas por faltas leves, al año. El plazo de prescripción de las sanciones comenzará a computarse desde el día siguiente a aquel en que sea ejecutable la resolución por la que se impone la sanción o haya transcurrido el plazo para recurrirla. Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento de ejecución, volviendo a correr el plazo si aquél está paralizado durante más de un mes por causa no imputable al infractor.

Artículo 114. *Competencias y procedimiento sancionador.*

1. La competencia sancionadora corresponderá:

a) a la Comisión Nacional de los Mercados y la Competencia, en el ámbito material de su actuación, cuando se trate de infracciones muy graves tipificadas en los apartados 3, 10, 11 y 14 del artículo 106, infracciones graves tipificadas en los apartados 19, 20, 24, 25, 27, 28, 34, 35, 36, 38, 39 y 41 del artículo 107 e infracciones leves tipificadas en los apartados 6 y 12 del artículo 108;

b) a la Agencia Española de Protección de Datos, en el caso de que se trate de las infracciones graves del artículo 107 tipificadas en el apartado 30 y de las infracciones leves del artículo 108 tipificadas en el apartado 11 cuando se vulneren los derechos de los usuarios finales sobre protección de datos y privacidad reconocidos en el artículo 66;

c) a la persona titular de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, el resto de los casos y en los supuestos de imposición de sanciones por la comisión de las infracciones señaladas en las letras a) y b) cuando se trate de su ámbito material de actuación.

2. En el ejercicio de la potestad sancionadora será de aplicación el procedimiento administrativo común establecido en la Ley 39/2015, de 1 de octubre, si bien el plazo de resolución del mismo será de un año y el plazo de alegaciones será como mínimo de quince días hábiles.

Disposición adicional primera. *Significado de los términos empleados por esta ley.*

A los efectos de esta ley, los términos definidos en el anexo II tendrán el significado que allí se les asigna.

Disposición adicional segunda. *Limitaciones y servidumbres.*

1. Las limitaciones a la propiedad y las servidumbres a las que hace referencia el artículo 47.1 podrán afectar:

a) a la altura máxima de los edificios;
b) a la distancia mínima a la que podrán ubicarse industrias que produzcan emisiones radioeléctricas e instalaciones eléctricas de alta tensión y líneas férreas electrificadas no soterradas;
c) a la distancia mínima a la que podrán instalarse transmisores radioeléctricos.

2. Con la excepción de la normativa legal vigente aplicable a la defensa nacional, a la navegación aérea y a la radioastronomía, no podrán establecerse, por vía reglamentaria, limitaciones a la propiedad ni servidumbres que contengan condiciones más gravosas que las siguientes:

a) para distancias inferiores a 1.000 metros, el ángulo sobre la horizontal con el que se observe, desde la parte superior de las antenas receptoras de menor altura de la estación, el punto más elevado de un edificio será como máximo de tres grados;
b) la máxima limitación exigible de separación entre una industria que produzca emisiones radioeléctricas o una línea de tendido eléctrico de alta tensión o líneas de ferrocarril no soterradas y cualquiera de las antenas receptoras de la estación será de 1.000 metros.

La instalación de transmisores radioeléctricos en las proximidades de la estación se realizará con las siguientes limitaciones:

Gama de frecuencias	Potencia radiada aparente del transmisor en dirección a la instalación a proteger – Kilovatios	Máxima limitación exigible de separación entre instalaciones a proteger y antena del transmisor – Kilómetros
f ≤ 30 MHz	0,01 < P ≤ 1	2
	1 < P ≤ 10	10
	P > 10	20
f > 30 MHz	0,01 < P ≤ 1	1
	1 < P ≤ 10	2
	P > 10	5

3. Las limitaciones de intensidad de campo eléctrico se exigirán para aquellas instalaciones cuyos equipos tengan una alta sensibilidad. Se entiende que utilizan equipos de alta sensibilidad las instalaciones dedicadas a la investigación:

a) las estaciones dedicadas a la observación radioastronómica, estas limitaciones serán las siguientes:

Niveles máximos admisibles de densidad espectral de flujo de potencia en las estaciones de observación de Radioastronomía [(1)(2)]			
Frecuencia central (MHz)	Anchura de banda de canal (kHz)	Densidad espectral de flujo de potencia (dB(W/(m2 · Hz)))	Observaciones radioastronómicas
13,385	50	-248	Continuo.
25,61	120	-249	Continuo.
73,8	1600	-258	Continuo.
151,525	2950	-259	Continuo.
325,3	6600	-258	Continuo.
327	10	-244	Rayas espectrales.
408,05	3900	-255	Continuo.
611	6000	-253	Continuo.
1413,5	27000	-255	Continuo.
1420	20	-239	Rayas espectrales.
1612	20	-238	Rayas espectrales.
1665	20	-237	Rayas espectrales.
1665	10000	-251	Continuo.
2695	10000	-247	Continuo.
4830	50	-230	Rayas espectrales.
4995	10000	-241	Continuo.
10650	100000	-240	Continuo.
14488	150	-221	Rayas espectrales.

(1) Los valores anteriores corresponden a una ganancia supuesta de la antena receptora de radioastronomía de 0 dBi.

(2) Para sistemas interferentes con condiciones de propagación variables en el tiempo los niveles dados no podrán ser excedidos en la medida en que la pérdida de datos supere el 2 %.

Niveles máximos admisibles de densidad espectral de flujo de potencia en las estaciones de observación de Radioastronomía [1][2]			
Frecuencia central (MHz)	Anchura de banda de canal (kHz)	Densidad espectral de flujo de potencia (dB(W/(m2 · Hz)))	Observaciones radioastronómicas
15375	50000	-233	Continuo.
22200	250	-216	Rayas espectrales.
22355	290000	-231	Continuo.
23700	250	-215	Rayas espectrales.
23800	400000	-233	Continuo.
31550	500000	-228	Continuo.
43000	500	-210	Rayas espectrales.
43000	1000000	-227	Continuo.
48000	500	-209	Rayas espectrales.
76750	8000000	-229	Continuo.
82500	8000000	-228	Continuo.
88600	1000	-208	Rayas espectrales.
89000	8000000	-228	Continuo.
105050	8000000	-223	Continuo.
132000	8000000	-223	Continuo.
147250	8000000	-223	Continuo.
150000	8000000	-223	Continuo.
150000	1000	-204	Rayas espectrales.
165500	8000000	-222	Continuo.
183500	8000000	-220	Continuo.
215750	8000000	-218	Continuo.
220000	1000	-199	Rayas espectrales.
224000	8000000	-218	Continuo.
244500	8000000	-217	Continuo.
265000	1000	-197	Rayas espectrales.
270000	8000000	-216	Continuo.

[1] Los valores anteriores corresponden a una ganancia supuesta de la antena receptora de radioastronomía de 0 dBi.

[2] Para sistemas interferentes con condiciones de propagación variables en el tiempo los niveles dados no podrán ser excedidos en la medida en que la pérdida de datos supere el 2 %.

b) para la protección de las instalaciones de observatorios de astrofísica, la limitación de la intensidad de campo eléctrico, en cualquier frecuencia, será de 88,8 dB (µV/m) en la ubicación del observatorio.

4. Para un mejor aprovechamiento del dominio público radioeléctrico, el Ministerio de Asuntos Económicos y Transformación Digital podrá imponer la utilización en las instalaciones de aquellos elementos técnicos que mejoren la compatibilidad radioeléctrica entre estaciones.

Disposición adicional tercera. *Aplicación de la legislación reguladora de las infraestructuras comunes en los edificios.*

Las infraestructuras comunes de telecomunicaciones en el interior de los edificios se regulan por lo establecido en la presente ley, por el Real Decreto-ley 1/1998, de 27 de febrero, sobre infraestructuras comunes en los edificios para el acceso a los servicios de telecomunicación y sus desarrollos reglamentarios.

Disposición adicional cuarta. *Información confidencial.*

Las personas físicas o jurídicas que aporten a alguna de las autoridades públicas competentes específicas en materia de telecomunicaciones datos o informaciones de cualquier tipo, con ocasión del desempeño de sus funciones y respetando la legislación vigente en materia de protección de datos y privacidad, podrán indicar, de forma justificada, qué parte de lo aportado consideran confidencial, cuya difusión podría perjudicarles, a los efectos de que sea declarada su confidencialidad. Cada autoridad pública competente específica en materia de telecomunicaciones decidirá, de forma motivada y a través de las resoluciones oportunas, sobre la información que, según la legislación vigente, resulte o no amparada por la confidencialidad.

Disposición adicional quinta. *Referencia a servicios de comunicaciones electrónicas en otras normas.*

Las referencias a los servicios de comunicaciones electrónicas efectuadas en otras normas previas a la vigencia del Código Europeo de Comunicaciones Electrónicas se entenderán realizadas a las distintas clases de servicios de comunicaciones electrónicas que

establece el citado Código (servicio de acceso a internet, servicio de comunicaciones interpersonales basado en la numeración, servicio de comunicaciones interpersonales independiente de la numeración y servicios consistentes, en su totalidad o principalmente, en el transporte de señales). En función de la naturaleza y características de cada servicio en concreto y de la finalidad que persiga dicha normativa, se tendrán en cuenta al efecto los derechos y obligaciones que el mencionado Código Europeo y la presente ley asocian a cada clase de servicio de comunicaciones electrónicas.

Disposición adicional sexta. *Multas coercitivas.*

Para asegurar el cumplimiento de las resoluciones o requerimientos de información que dicten el Ministerio de Asuntos Económicos y Transformación Digital o la Comisión Nacional de los Mercados y la Competencia podrán imponer multas coercitivas por importe diario de 125 hasta 30.000 euros, en los términos previstos en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Las multas coercitivas serán independientes de las sanciones que puedan imponerse y compatibles con ellas.

El importe de las multas coercitivas previstas en esta disposición se ingresará en el Tesoro Público.

Disposición adicional séptima. *Obligaciones en materia de acceso condicional, acceso a determinados servicios de comunicación audiovisual televisivos y radiofónicos y obligaciones de transmisión.*

1. En el acceso condicional a los servicios digitales de comunicación audiovisual televisivos y radiofónicos difundidos a los telespectadores y oyentes, deberán cumplirse los requisitos siguientes, con independencia del medio de transmisión utilizado:

a) con independencia de los medios de transmisión, todas las empresas proveedoras de servicios de acceso condicional que prestan servicios de acceso a los servicios digitales de comunicación audiovisual televisivos y radiofónicos y de cuyos servicios de acceso dependen los prestadores del servicio de comunicación audiovisual para llegar a cualquier grupo de telespectadores u oyentes potenciales estarán obligados a:

1.º proponer a todos los prestadores del servicio de comunicación audiovisual, en condiciones equitativas, razonables y no discriminatorias que resulten compatibles con el Derecho de la competencia, servicios técnicos que permitan que sus servicios digitales de comunicación audiovisual televisivos y radiofónicos sean recibidos por los telespectadores u oyentes autorizados, mediante descodificadores gestionados por los operadores de servicios, así como a respetar el Derecho de la competencia;

2.º llevar una contabilidad financiera separada en lo que se refiere a su actividad de suministro de servicios de acceso condicional;

b) cuando concedan licencias a los fabricantes de equipos de consumo, los titulares de los derechos de propiedad industrial relativos a los sistemas y productos de acceso condicional, deberán hacerlo en condiciones equitativas, razonables y no discriminatorias. La concesión de licencias, que tendrá en cuenta los factores técnicos y comerciales, no podrá estar subordinada por los propietarios de los derechos a condiciones que prohíban, disuadan o desalienten la inclusión en el mismo producto de:

1.º bien una interfaz común que permita la conexión con varios sistemas de acceso;

2.º bien medios específicos de otro sistema de acceso, siempre que el beneficiario de la licencia respete las condiciones razonables y apropiadas que garanticen, por lo que a él se refiere, la seguridad de las transacciones de los operadores de sistemas de acceso condicional.

2. En el caso de que en el mercado involucrado en el acceso condicional a los servicios digitales de comunicación audiovisual televisivos y radiofónicos no se hubiera designado operador con peso significativo en el mercado, la Comisión Nacional de los Mercados y la Competencia podrá modificar o suprimir las condiciones con respecto a los operadores de dicho mercado, siempre y cuando:

a) dicha modificación o supresión no incida negativamente en el acceso de los usuarios finales a las emisiones de los servicios de comunicación audiovisual televisivos y radiofónicos, y

b) dicha modificación o supresión no incida negativamente en las perspectivas de competencia efectiva en los siguientes mercados:

1.º los mercados de servicios de comunicación audiovisual al por menor de radio y televisión digital;

2.º los mercados de sistemas de acceso condicional y otros recursos asociados.

3. Mediante orden de la persona titular del Ministerio de Asuntos Económicos y Transformación Digital se podrá imponer exigencias razonables de transmisión de determinados canales de servicios de comunicación audiovisual televisivos y radiofónicos, así como exigencias de transmisión de servicios complementarios para posibilitar el acceso adecuado de los usuarios con discapacidad, a los operadores que exploten redes de comunicaciones electrónicas utilizadas para la distribución de servicios de comunicación audiovisual al público, si un número significativo de usuarios finales de dichas redes las utiliza como medio principal de recepción de programas de servicios de comunicación audiovisual, cuando resulte necesario para alcanzar objetivos de interés general claramente definidos y de forma proporcionada, transparente y periódicamente revisable.

Asimismo, podrán establecerse mediante real decreto condiciones a los proveedores de servicios y equipos de televisión digital, para que cooperen en la prestación de servicios de comunicación audiovisual televisiva interoperables para los usuarios finales con discapacidad.

4. Mediante orden de la persona titular del Ministerio de Asuntos Económicos y Transformación Digital se regulará el establecimiento de las obligaciones y requisitos para los gestores de múltiples digitales de la televisión digital terrestre y la creación y regulación del Registro de parámetros de información de los servicios de televisión digital terrestre. La gestión, asignación y control de los parámetros de información de los servicios de televisión digital terrestre y la llevanza de dicho Registro corresponde a la Comisión Nacional de los Mercados y la Competencia.

Disposición adicional octava. *Interoperabilidad de receptores de servicios de comunicación audiovisual radiofónicos para automóviles, de receptores de servicios de comunicación audiovisual radiofónicos de consumo y equipos de consumo utilizados para la televisión digital.*

1. Los equipos receptores de servicios de comunicación audiovisual radiofónicos para automóviles y los equipos de consumo utilizados para la televisión digital deben ser interoperables de conformidad con las siguientes reglas:

a) algoritmo de cifrado común y recepción de libre acceso. Todos los equipos de consumo para la recepción de señales de televisión digital, ya sea por emisión terrestre, por cable o por satélite, que se comercialicen para la venta, en alquiler o en cualquier otra fórmula comercial con capacidad para descifrar señales de televisión digital deberán incluir las siguientes funciones:

i) descifrado de señales de conformidad con un algoritmo de cifrado común europeo gestionado por una organización europea de normalización reconocida;

ii) visualización de señales transmitidas en abierto, a condición de que, en los casos en que el equipo se suministre en alquiler, el arrendatario se halle en situación de cumplimiento del contrato correspondiente;

b) interoperabilidad de aparatos de televisión digitales. Todo aparato digital de televisión dotado de una pantalla de visualización integral de una diagonal visible superior a 30 centímetros comercializado para su venta o alquiler deberá estar provisto de, al menos, una conexión de interfaz abierta normalizada por una organización europea de normalización reconocida, conforme con la norma adoptada por ésta, o conforme con las especificaciones adoptadas por la industria, que permita la conexión sencilla de periféricos, y poder transferir todos los elementos pertinentes de una señal de televisión digital, incluida la información relativa a servicios interactivos y de acceso condicional;

c) interoperabilidad de los receptores de servicios de radio para automóviles. Todo receptor de servicios de radio integrado en un vehículo nuevo de la categoría M introducido en el mercado para su venta o alquiler deberá incluir un receptor capaz de recepción y reproducción de, al menos, los servicios de radiodifusión ofrecidos a través de la radiodifusión digital terrestre.

Lo establecido en el presente apartado podrá ser objeto de modificación mediante real decreto, de conformidad con lo que dispongan las normas y actos emanados de las instituciones europeas.

2. Mediante real decreto se podrán adoptar medidas para garantizar la interoperabilidad de otros receptores de servicios de radio de consumo, para lo cual deberá tenerse en cuenta el impacto en el mercado de los receptores de radiodifusión de valor reducido y garantizar que dichas medidas no se apliquen a los productos en los que el receptor de servicios de radio tenga un carácter puramente auxiliar, como los teléfonos móviles multifunción, ni a los equipos utilizados por radioaficionados.

3. Los usuarios finales, en el momento de la resolución de su contrato, tendrán la posibilidad de devolver los equipos terminales de televisión digital de forma gratuita y sencilla, a menos que el proveedor demuestre la completa interoperabilidad del equipo con los servicios de televisión digital de otros proveedores, entre ellos aquel al que se haya cambiado el usuario final.

Mediante real decreto se podrán adoptar medidas para que los equipos terminales de televisión digital que los prestadores de servicios digitales de televisión suministren a sus usuarios finales sean interoperables a fin de que, cuando ello sea técnicamente posible, estos puedan reutilizarse con otros prestadores de servicios digitales de televisión. En todo caso, se considerará que los equipos terminales de televisión digital que sean conformes a las normas armonizadas cuyas referencias hayan sido publicadas en el «Diario Oficial de la Unión Europea», o a partes de estas, cumplen el requisito de interoperabilidad establecido en este párrafo.

Disposición adicional novena. *Mecanismo de notificación.*

Las medidas adoptadas por la Comisión Nacional de los Mercados y la Competencia de acuerdo con los capítulos III, IV y V del título II, artículo 55.8 y disposición adicional séptima de esta ley, y su normativa de desarrollo, que puedan tener repercusiones en los intercambios entre Estados miembros, se someterán a los mecanismos de notificación a que se refieren los artículos 32, 33 y 34 del Código Europeo de Comunicaciones Electrónicas y las normas dictadas al efecto en desarrollo de los mismos por la Unión Europea.

Disposición adicional décima. *Mecanismo de consulta.*

Las autoridades públicas competentes específicas en materia de telecomunicaciones que tengan la intención de adoptar medidas conforme a lo establecido en la presente ley y su normativa de desarrollo que incidan significativamente en el mercado pertinente así como medidas de restricción a la neutralidad tecnológica y de servicios en el uso del dominio público radioeléctrico regulada en el artículo 93, deberán dar a los interesados la oportunidad de formular observaciones sobre la medida propuesta en un plazo razonable, según la complejidad del asunto, pero en cualquier caso no inferior a treinta días naturales, excepto en circunstancias excepcionales, en los términos y con las condiciones establecidas en el artículo 23 del Código Europeo de Comunicaciones Electrónicas y las normas dictadas al efecto en desarrollo del mismo por la Unión Europea.

Disposición adicional undécima. *Informe sobre las obligaciones a imponer a operadores de redes públicas o de servicios de comunicaciones electrónicas disponibles al público.*

Cualquier medida normativa que vaya a aprobarse con posterioridad a la entrada en vigor de la presente ley o acto administrativo en ejecución de dicha medida normativa que tramite cualquier Administración Pública y que persiga imponer con carácter generalizado a los operadores de redes públicas o de servicios de comunicaciones electrónicas disponibles al público o a un grupo específico de los mismos obligaciones de servicio público distintas de las previstas en el artículo 43, obligaciones de supervisión de la información tratada o

gestionada en dichas redes o servicios o de colaboración con los agentes facultados respecto al tráfico gestionado, requerirá el informe preceptivo del Ministerio de Asuntos Económicos y Transformación Digital.

Dicha medida normativa o acto administrativo deberá contemplar de manera expresa los mecanismos de financiación de los costes derivados de las obligaciones de servicio público distintas de las previstas en el artículo 43, obligaciones de carácter público o cualquier otra carga administrativa que se imponga, que no podrá ser a cargo de los operadores de redes públicas o de servicios de comunicaciones electrónicas disponibles al público cuando se traten de obligaciones o cargas que no deriven directamente del marco normativo de las comunicaciones electrónicas sino que respondan a otras razones de políticas públicas, salvo que concurran motivos de interés público que lleven a la conclusión de que dichos operadores deban asumir dichos costes, aun cuando sea parcialmente.

La solicitud del preceptivo informe del Ministerio de Asuntos Económicos y Transformación Digital se considera un requisito esencial en la tramitación de la norma o acto administrativo.

Disposición adicional duodécima. *Creación de la Comisión sobre radiofrecuencias y salud.*

Mediante real decreto se regulará la composición, organización y funciones de la Comisión sobre radiofrecuencias y salud, cuya misión es la de asesorar e informar a la ciudadanía, al conjunto de las Administraciones públicas y a los diversos agentes de la industria sobre las restricciones establecidas a las emisiones radioeléctricas, las medidas de protección sanitaria aprobadas frente a emisiones radioeléctricas y los múltiples y periódicos controles a que son sometidas las instalaciones generadoras de emisiones radioeléctricas, en particular, las relativas a las radiocomunicaciones. Asimismo, dicha Comisión realizará y divulgará estudios e investigaciones sobre las emisiones radioeléctricas y sus efectos y cómo las restricciones a las emisiones, las medidas de protección sanitaria y los controles establecidos preservan la salud de las personas, así como, a la vista de dichos estudios e investigaciones, realizará propuestas y sugerirá líneas de mejora en las medidas y controles a realizar.

De la Comisión formarán parte en todo caso el Ministerio de Asuntos Económicos y Transformación Digital, el Ministerio de Sanidad y el Instituto de Salud Carlos III y una representación de las Comunidades Autónomas.

Dicha Comisión contará con un grupo asesor o colaborador en materia de radiofrecuencias y salud, con participación de Comunidades Autónomas, de la asociación de entidades locales de ámbito estatal con mayor implantación y un grupo de expertos independientes, sociedades científicas y representantes de los ciudadanos, para hacer evaluación y seguimiento periódico de la prevención y protección de la salud de la población en relación con las emisiones radioeléctricas, proponiendo estudios de investigación, medidas consensuadas de identificación, elaboración de registros y protocolos de atención al ciudadano.

La creación y el funcionamiento tanto de la Comisión como del grupo asesor se atenderán con los medios personales, técnicos y presupuestarios actuales asignados a los Ministerios y demás Administraciones participantes, sin incremento en el gasto público.

Disposición adicional decimotercera. *Parámetros y requerimientos técnicos esenciales para garantizar el funcionamiento de las distintas redes y servicios de comunicaciones electrónicas.*

Los parámetros y requerimientos técnicos esenciales que son indispensables para garantizar el funcionamiento de las redes y servicios de comunicaciones electrónicas se establecerán mediante real decreto aprobado en Consejo de Ministros.

Disposición adicional decimocuarta. *Cooperación en la promoción de contenidos lícitos en redes y servicios de comunicaciones electrónicas.*

Las autoridades competentes podrán promover la cooperación entre los operadores de redes o servicios de comunicaciones electrónicas y los sectores interesados en la promoción de contenidos lícitos en dichas redes y servicios.

Disposición adicional decimoquinta. *Garantía de los derechos digitales.*

Lo dispuesto en esta ley será sin perjuicio de la aplicación de las medidas que en materia de garantía de los derechos digitales se establecen en el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016 y en el título X de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Disposición adicional decimosexta. *Políticas de impulso de los derechos digitales.*

El Gobierno, en colaboración con las Comunidades Autónomas, elaborará un Plan de Acceso a Internet con los siguientes objetivos:

a) superar las brechas digitales y garantizar el acceso a internet de los colectivos vulnerables o con necesidades especiales y de entornos familiares y sociales económicamente desfavorecidos;

b) impulsar la existencia de espacios de conexión de acceso público y

c) fomentar medidas educativas que promuevan la formación en competencias y habilidades digitales básicas de las personas y colectivos en riesgo de exclusión digital y la capacidad de todas las personas para realizar un uso autónomo y responsable de internet y de las tecnologías digitales.

Disposición adicional decimoséptima. *Coordinación de las ayudas públicas a la banda ancha y al desarrollo de la economía y empleo digitales y nuevos servicios digitales.*

Por real decreto se identificarán los órganos competentes y se establecerán los procedimientos de coordinación entre Administraciones y Organismos públicos, en relación con las ayudas públicas a la banda ancha, cuya convocatoria y otorgamiento deberá respetar en todo caso el marco comunitario y los objetivos estipulados en el artículo 3 y en relación con el fomento de la I + D + I y a las actuaciones para el desarrollo de la economía, el empleo digital y todos los nuevos servicios digitales que las nuevas redes de alta y muy alta capacidad permiten, garantizando la cohesión social y territorial.

Disposición adicional decimoctava. *Publicación de actos.*

Los actos que formen parte de las distintas fases de los procedimientos que tramite el Ministerio de Asuntos Económicos y Transformación Digital y la Comisión Nacional de los Mercados y la Competencia en el ejercicio de las competencias y funciones asignadas en las materias a que se refiere la presente ley se podrán publicar en el «Boletín Oficial del Estado», de conformidad con lo previsto en el artículo 45 y disposición adicional tercera de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. En particular, todas aquellas resoluciones, actos administrativos o actos de trámite dictados por el Ministerio de Asuntos Económicos y Transformación Digital y la Comisión Nacional de los Mercados y la Competencia en el ejercicio de las competencias y funciones asignadas en las materias a que se refiere la presente ley y que pudieran tener por destinatario a una pluralidad indeterminada de personas o cuando estime que la notificación efectuada a un solo interesado es insuficiente para garantizar la notificación a todos, deberán ser publicados en el «Boletín Oficial del Estado», de conformidad con lo previsto en el artículo 45.1.a) de la Ley 39/2015, de 1 de octubre.

Disposición adicional decimonovena. *Estaciones radioeléctricas de radioaficionado.*

En la instalación de estaciones radioeléctricas de radioaficionado se aplicará lo establecido en el primer párrafo del artículo 49.9, sin perjuicio de la aplicación de la Ley

19/1983, de 16 de noviembre, sobre regulación del derecho a instalar en el exterior de los inmuebles las antenas de las estaciones radioeléctricas de aficionados, y su normativa de desarrollo.

Disposición adicional vigésima. *Prestación de determinados servicios a los que se refiere el artículo 43.*

La Dirección General de la Marina Mercante asume la prestación de los servicios de seguridad de la vida humana en el mar subsumibles bajo el artículo 43.1.

Disposición adicional vigésima primera. *Comunicación al Registro de operadores de los prestadores del servicio de comunicaciones electrónicas interpersonales independientes de la numeración disponible al público.*

Los operadores que estén prestando el servicio de comunicaciones electrónicas interpersonales independientes de la numeración disponible al público dispondrán del plazo de dos meses a contar desde la entrada en vigor de esta ley para efectuar la comunicación al Registro de operadores a que se refiere el artículo 6.6.

En la comunicación se deberá proporcionar la siguiente información mínima:

a) nombre y apellidos o, en su caso, denominación o razón social y nacionalidad del operador;

b) datos de inscripción en el registro mercantil u otro registro público similar en el que figure el operador y número de identificación fiscal;

c) domicilio social y el señalado a los efectos de notificaciones;

d) el sitio web del proveedor, de haberlo, asociado al suministro de servicios de comunicaciones electrónicas;

e) nombre, apellidos, número de documento nacional de identidad o pasaporte de su representante y de la persona responsable a los efectos de notificaciones, incluyendo, respecto a esta última, la dirección de correo electrónico y número de teléfono móvil para poder recibir los avisos de puesta a disposición de las notificaciones que le sean enviadas;

f) una exposición sucinta de los servicios que suministra.

Disposición adicional vigésima segunda. *Comunicación al Ministerio de Asuntos Económicos y Transformación Digital de los puntos de intercambio de internet (IXP).*

Los titulares y gestores de los puntos de intercambio de internet (IXP) ubicados en territorio español dispondrán del plazo de dos meses a contar desde la entrada en vigor de esta ley para efectuar la comunicación al Ministerio de Asuntos Económicos y Transformación Digital a que se refiere el artículo 6.8.

En la comunicación se deberá proporcionar la siguiente información mínima:

a) nombre y apellidos o, en su caso, denominación o razón social y nacionalidad del titular y del gestor del punto de intercambio de internet (IXP);

b) datos de inscripción en el registro mercantil u otro registro público similar en el que figure el titular y el gestor del punto de intercambio de internet (IXP) y número de identificación fiscal;

c) domicilio social y el señalado a los efectos de notificaciones;

d) el sitio web del titular y del gestor del punto de intercambio de internet (IXP), de haberlo;

e) nombre, apellidos, número de documento nacional de identidad o pasaporte de su representante y de la persona responsable a los efectos de notificaciones, incluyendo, respecto a esta última la dirección de correo electrónico y número de teléfono móvil para poder recibir los avisos de puesta a disposición de las notificaciones que le sean enviadas;

f) ubicación de cada uno de los puntos de intercambio de internet (IXP) de los que sea titular o gestor y una exposición sucinta de sus principales características técnicas.

Disposición adicional vigésima tercera. *Comunicación al Ministerio de Asuntos Económicos y Transformación Digital de los cables submarinos.*

Los titulares y gestores de cables submarinos cuyo enganche, acceso o interconexión a redes de comunicaciones electrónicas se produce en territorio español, dispondrán del plazo de dos meses a contar desde la entrada en vigor de esta ley para efectuar la comunicación a que se refiere el artículo 6.9.

En la comunicación se deberá proporcionar la siguiente información mínima:

a) nombre y apellidos o, en su caso, denominación o razón social y nacionalidad del titular y del gestor del cable submarino;

b) datos de inscripción en el registro mercantil u otro registro público similar en el que figure el titular y el gestor del cable submarino y número de identificación fiscal;

c) domicilio social y el señalado a los efectos de notificaciones;

d) el sitio web del titular y del gestor del cable submarino, de haberlo;

e) nombre, apellidos, número de documento nacional de identidad o pasaporte de su representante y de la persona responsable a los efectos de notificaciones, incluyendo, respecto a esta última, la dirección de correo electrónico y número de teléfono móvil para poder recibir los avisos de puesta a disposición de las notificaciones que le sean enviadas;

f) una exposición sucinta del trazado del cable submarino y de sus principales características técnicas y, en particular, del lugar en el que se produce el enganche, acceso o interconexión a redes de comunicaciones electrónicas ubicadas en territorio español.

Disposición adicional vigésima cuarta. *Reconversión de la infraestructura de los teléfonos públicos de pago.*

Las infraestructuras de los teléfonos públicos de pago se podrán reconvertir o utilizar como puntos de conectividad para la prestación, entre otros, de los siguientes servicios:

a) puntos de conexión a internet;

b) teléfono de emergencias;

c) punto de envío y recogida de paquetería.

Disposición adicional vigésima quinta. *Datos del Registro de operadores puestos a disposición del ORECE.*

Los datos correspondientes a las notificaciones efectuadas al Registro de operadores que hayan sido inscritos entre el 21 de diciembre de 2020 y la entrada en vigor de esta ley deberán ponerse a disposición del ORECE a la mayor brevedad posible.

Disposición adicional vigésima sexta. *Reasignación de recursos.*

Los órganos y organismos de la Administración General del Estado podrán ejercer las funciones que en la presente ley se les atribuyen con sus recursos disponibles sin necesidad de requerir dotaciones presupuestarias adicionales.

Disposición adicional vigésima séptima. *Adaptación de la contratación con los usuarios finales por los operadores de comunicaciones electrónicas.*

1. Los operadores de comunicaciones electrónicas dispondrán de un plazo de dos meses a contar desde la entrada en vigor de esta ley para adaptar su operativa y el contenido de los contratos a formalizar con los usuarios finales a lo establecido en el capítulo IV del título III y demás disposiciones de esta ley.

2. Los operadores de comunicaciones electrónicas dispondrán de un plazo de cuatro meses a contar desde la entrada en vigor de esta ley para modificar los contratos formalizados con los usuarios finales para adaptarlos a lo establecido en el capítulo IV del título III y demás disposiciones de esta ley o, en su caso, y a petición expresa de los usuarios, proceder a su rescisión en los términos indicados en el artículo 67.8.

Disposición adicional vigésima octava. *Creación de la Comisión Interministerial para la agilización de los mecanismos de colaboración entre Administraciones públicas para la instalación y explotación de las redes públicas de comunicaciones electrónicas.*

Mediante real decreto se regulará la composición, organización y funciones de la Comisión Interministerial para la agilización de los mecanismos de colaboración entre Administraciones públicas para la instalación y explotación de las redes públicas de comunicaciones electrónicas, cuya misión es el impulso de la resolución ágil y eficiente de las solicitudes de ocupación del dominio público y la propiedad privada presentadas por los operadores ante las diferentes Administraciones públicas al amparo del artículo 49 de la presente ley, garantizando el cumplimiento de los plazos legalmente establecidos y minimizando los retrasos y las incidencias asociadas a la tramitación y resolución de dichas solicitudes de ocupación. De la Comisión Interministerial formarán parte en todo caso el Ministerio de Asuntos Económicos y Transformación Digital, el Ministerio de Transportes, Movilidad y Agenda Urbana y el Ministerio para la Transición Ecológica y el Reto Demográfico.

Disposición adicional vigésima novena. *Beneficios fiscales aplicables al evento «Año Santo Jubilar San Isidro Labrador».*

1. La celebración del «Año Santo Jubilar San Isidro Labrador» tendrá la consideración de acontecimiento excepcional de interés público a los efectos de lo dispuesto en el artículo 27 de la Ley 49/2002, de 23 de diciembre, de régimen fiscal de las entidades sin fines lucrativos y de los incentivos fiscales al mecenazgo.
2. La duración del programa de apoyo a este acontecimiento abarcará desde la entrada en vigor de la presente ley al 15 de mayo de 2023.
3. La certificación de la adecuación de los gastos realizados a los objetivos y planes del programa se efectuará de conformidad con lo dispuesto en la citada Ley 49/2002, de 23 de diciembre.
4. Las actuaciones a realizar serán las que aseguren el adecuado desarrollo del acontecimiento. El desarrollo y concreción en planes y programas de actividades específicas se realizarán por el órgano competente de conformidad con lo dispuesto en el citada Ley 49/2002, de 23 de diciembre.
5. Los beneficios fiscales de este programa serán los máximos establecidos en el artículo 27.3 de la citada Ley 49/2002, de 23 de diciembre.

Disposición adicional trigésima. *Universalización del acceso a internet a una velocidad mínima de 100 Mbit por segundo.*

El Gobierno desarrollará las medidas adecuadas que tengan como objetivo lograr en el plazo de un año a contar desde la entrada en vigor de esta ley la universalización del acceso a internet de banda ancha a una velocidad mínima de 100 Mbit por segundo en sentido descendente y, adicionalmente, que dicho acceso se produzca a unos precios asequibles para los ciudadanos, con independencia de su localización geográfica, en aras de impulsar la cohesión social y territorial mediante el despliegue de las más modernas redes de telecomunicaciones que posibilite el acceso de los ciudadanos a los más diversos y necesarios servicios, cada vez más básicos y esenciales, que se prestan a través de estas redes, como el teletrabajo, la telemedicina o la enseñanza online, y con ello fortalecer la vertebración social y territorial, coadyuvando al objetivo de afrontar el reto demográfico y de ayudar a la fijación de la población en el territorio, combatiendo la despoblación rural.

Disposición transitoria primera. *Normativa anterior a la entrada en vigor de esta ley.*

Las normas reglamentarias en materia de telecomunicaciones vigentes con anterioridad a la entrada en vigor de la presente ley o dictadas en desarrollo de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones o de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, continuarán vigentes en lo que no se opongan a esta ley, hasta que se apruebe su normativa de desarrollo.

Disposición transitoria segunda. *Adaptación de los títulos habilitantes del uso del dominio público radioeléctrico.*

1. Los títulos habilitantes del uso del dominio público radioeléctrico otorgados con anterioridad a la entrada en vigor de la presente ley quedan automáticamente adaptados al régimen jurídico establecido en ésta, a excepción de su duración, que será la establecida en el título original o sus modificaciones.

2. Los títulos habilitantes del uso privativo del dominio público radioeléctrico con limitación de número otorgados mediante procedimientos de licitación y cuyo otorgamiento siga siendo con limitación de número podrán ver ampliada su duración hasta un plazo total de cuarenta años, incluidas prórrogas y modificaciones, si bien la ampliación de plazo no podrá en ningún caso ser superior a los diez años adicionales a la duración actual del título habilitante, incluidas prórrogas y modificaciones. Asimismo, estos títulos habilitantes podrán ser objeto de renovación en los términos indicados en el artículo 94.7.

Esta adaptación en los plazos de duración y en la posible renovación de los títulos habilitantes mencionados se aprobará mediante orden de la persona titular del Ministerio de Asuntos Económicos y Transformación Digital, en la que se tendrán en cuenta las circunstancias particulares de cada banda de frecuencias y de cada título habilitante, incluidas sus modificaciones, previa solicitud del titular del título habilitante, que deberá ser presentada en el plazo de dos meses a contar desde la entrada en vigor de esta ley.

En la tramitación de la orden ministerial se evacuará un trámite de audiencia con el titular solicitante y se dará a todas las partes interesadas la oportunidad de manifestar su punto de vista a través de un procedimiento público de consulta conforme con lo dispuesto en la disposición adicional décima. Asimismo, se solicitará el informe previo de la Comisión Nacional de los Mercados y la Competencia e informe de la Abogacía del Estado.

Disposición transitoria tercera. *Condiciones ligadas a las concesiones de uso de dominio público radioeléctrico.*

Las condiciones ligadas a los títulos habilitantes para la explotación de redes o prestación de servicios de telecomunicaciones que implicaran el uso del dominio público radioeléctrico y que se hubieran otorgado con anterioridad a la entrada en vigor de la presente ley a través de procedimientos de licitación pública, ya estuvieran previstas en los pliegos reguladores de las licitaciones o en la oferta del operador, pasan a estar ligadas a las concesiones de uso privativo de dominio público radioeléctrico.

Disposición transitoria cuarta. *Registro de operadores.*

El Registro de operadores regulado en el artículo 7 mantiene su continuidad respecto del Registro de operadores regulado en el artículo 7 de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, de manera que los datos inscritos en este pasarán a formar parte del registro regulado en esta ley.

Disposición transitoria quinta. *Prestación transitoria del servicio universal.*

Telefónica de España, S.A.U. seguirá encargándose de la prestación de los elementos de servicio universal relativos al suministro de la conexión a la red pública de comunicaciones electrónicas y a la prestación del servicio telefónico disponible al público en las mismas condiciones establecidas en la Orden ECE/1280/2019, de 26 de diciembre, por la que se designa a dicho operador como encargado de la prestación citada, hasta que finalice el plazo para el que fue designado o se proceda a efectuar una nueva designación de operador u operadores encargados de la prestación de los servicios incluidos en el servicio universal conforme al régimen jurídico instaurado por la presente ley y su normativa de desarrollo.

Disposición transitoria sexta. *Planes de precios del servicio universal.*

En tanto no se determine reglamentariamente, el abono social a los servicios de comunicaciones vocales a través de una conexión subyacente en una ubicación fija, el plan de precios aplicable a abonados invidentes o con graves dificultades visuales y el plan de

precios aplicable a usuarios sordos o con graves dificultades auditivas estarán definidos por los supuestos, requisitos y condiciones establecidos en el apartado 4 del anexo del Acuerdo de la Comisión Delegada del Gobierno para Asuntos Económicos de 25 de enero de 2007, publicado por Orden PRE/531/2007, de 5 de marzo, por el que se aprueban las condiciones para garantizar la asequibilidad de las ofertas aplicables a los servicios incluidos en el servicio universal, y el Acuerdo de la Comisión Delegada del Gobierno para Asuntos Económicos de 13 de mayo de 2010, por el que se modifica el umbral de renta familiar que da acceso al abono social, publicado por la Orden PRE/1619/2010, de 14 de junio.

Disposición transitoria séptima. *Régimen transitorio para la fijación de las tasas establecidas en el anexo I de esta ley.*

Hasta que por la Ley de Presupuestos Generales del Estado se fijen las cuantías de la tasa prevista en el apartado 4 del anexo I, se aplicarán las siguientes:

a) por la expedición de certificaciones registrales, 43,80 euros;
b) por la expedición de certificaciones de presentación a la administración de las telecomunicaciones del proyecto técnico de infraestructuras comunes de telecomunicaciones, el acta de replanteo, el boletín de instalación y el protocolo de pruebas y, en su caso, el certificado de fin de obra y sus anexos, 43,80 euros;
c) por la expedición de certificaciones de cumplimiento de especificaciones técnicas de equipos de telecomunicación, 345,65 euros;
d) por cada acto de inspección previa o comprobación técnica efectuado, 363,42 euros;
e) por la presentación de cada certificación expedida por técnico competente sustitutiva del acto de inspección previa, 90,67 euros;
f) por la tramitación de concesión demanial o autorización para el uso privativo o de autorización general para el uso especial del dominio público radioeléctrico, 70,53 euros;
g) por la tramitación de la autorización individual para el uso especial del dominio público radioeléctrico, 114,36 euros;
h) por la presentación a los exámenes de capacitación para operar estaciones de radioaficionado, 23,67 euros;
i) por inscripción en el registro de empresas instaladoras de telecomunicación, 107,72;
j) por la solicitud y emisión del dictamen técnico de evaluación de la conformidad de equipos de telecomunicación, 356,30 euros.

Disposición derogatoria única. *Derogación normativa.*

Sin perjuicio de lo dispuesto en las disposiciones transitorias, quedan derogadas las siguientes disposiciones:

a) la Ley 9/2014, de 9 mayo, General de Telecomunicaciones, a excepción de su disposición adicional decimosexta y las disposiciones transitorias séptima, novena y duodécima. No obstante, la derogación de las disposiciones finales primera, segunda, tercera, cuarta, quinta y séptima de la Ley 9/2014, de 9 de mayo, no afectará a los contenidos de las normas legales modificadas por las mismas, que se mantienen en sus términos actualmente vigentes;
b) la disposición adicional tercera de la Ley 12/2012, de 26 de diciembre, de medidas urgentes de liberalización del comercio y de determinados servicios;
c) igualmente, quedan derogadas cuantas otras disposiciones de igual o inferior rango se opongan a lo dispuesto en esta ley.

Disposición final primera. *Modificación de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.*

Se introducen las siguientes modificaciones en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas:

Uno. El artículo 9.2.c) queda redactado como sigue:

> «c) Cualquier otro sistema que las Administraciones públicas consideren válido en los términos y condiciones que se establezca, siempre que cuenten con un registro

previo como usuario que permita garantizar su identidad y previa comunicación a la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital. Esta comunicación vendrá acompañada de una declaración responsable de que se cumple con todos los requisitos establecidos en la normativa vigente. De forma previa a la eficacia jurídica del sistema, habrán de transcurrir dos meses desde dicha comunicación, durante los cuales el órgano estatal competente por motivos de seguridad pública podrá acudir a la vía jurisdiccional, previo informe vinculante de la Secretaría de Estado de Seguridad, que deberá emitir en el plazo de diez días desde su solicitud.»

Dos. El artículo 10.2.c) queda redactado como sigue:

«c) Cualquier otro sistema que las Administraciones públicas consideren válido en los términos y condiciones que se establezca, siempre que cuenten con un registro previo como usuario que permita garantizar su identidad y previa comunicación a la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital. Esta comunicación vendrá acompañada de una declaración responsable de que se cumple con todos los requisitos establecidos en la normativa vigente. De forma previa a la eficacia jurídica del sistema, habrán de transcurrir dos meses desde dicha comunicación, durante los cuales el órgano estatal competente por motivos de seguridad pública podrá acudir a la vía jurisdiccional, previo informe vinculante de la Secretaría de Estado de Seguridad, que deberá emitir en el plazo de diez días desde su solicitud.»

Tres. Se añade una nueva disposición adicional séptima que queda redactada como sigue:

«Disposición adicional séptima.

La Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital informará a la Conferencia Sectorial para asuntos de Seguridad Nacional de las resoluciones denegatorias de la autorización prevista en los artículos 9.2.c) y 10.2.c) de esta ley, que, en su caso, se hayan dictado en el plazo máximo de tres meses desde la adopción de la citada resolución.»

Disposición final segunda. *Títulos competenciales.*

Esta ley se dicta al amparo de la competencia exclusiva estatal en materia de telecomunicaciones, prevista en el artículo 149.1.21.ª de la Constitución. Asimismo, las disposiciones de la ley dirigidas a garantizar la unidad de mercado en el sector de las telecomunicaciones, se dictan al amparo del artículo 149.1.1.ª de la Constitución, sobre regulación de las condiciones básicas que garanticen la igualdad de todos los españoles en el ejercicio de los derechos y en el cumplimiento de los deberes constitucionales y del artículo 149.1.13.ª de la Constitución, sobre bases y coordinación de la planificación general de la actividad económica. Por último, las disposiciones del título VIII se dictan al amparo de la competencia exclusiva estatal en materia de hacienda general, prevista en el artículo 149.1.14.ª de la Constitución.

Disposición final tercera. *Regulación de las condiciones en que los órganos o entes gestores de infraestructuras de transporte de competencia estatal permitirán la ocupación del dominio público que gestionan y de la propiedad privada de que son titulares.*

A los efectos de lo previsto en los artículos 44 y 45, mediante real decreto acordado en Consejo de Ministros, a propuesta conjunta del Ministerio de Asuntos Económicos y Transformación Digital y del Ministerio de Transportes, Movilidad y Agenda Urbana, se determinarán las condiciones en que los órganos o entes gestores de infraestructuras de transporte de competencia estatal deben permitir el ejercicio del derecho de ocupación del dominio público que gestionan y de la propiedad privada de que son titulares, por los operadores de redes públicas y servicios de comunicaciones electrónicas disponibles al público bajo los principios del acceso efectivo a dichos bienes, la reducción de cargas, y la

simplificación administrativa, en condiciones equitativas, no discriminatorias, objetivas y neutrales.

Disposición final cuarta. *Incorporación de derecho de la Unión Europea.*

1. Mediante esta ley se incorporan al derecho español las siguientes Directivas:

a) Directiva 2018/1972, de 11 de diciembre de 2018, del Parlamento Europeo y del Consejo, por la que se establece el Código Europeo de las Comunicaciones Electrónicas.
b) Directiva 2014/61/UE, del Parlamento Europeo y del Consejo, de 15 de mayo de 2014, relativa a medidas para reducir el coste del despliegue de las redes de comunicaciones electrónicas de alta velocidad.
c) Directiva 2014/53/UE, del Parlamento Europeo y del Consejo, de 16 de abril de 2014, relativa a la armonización de las legislaciones de los Estados miembros sobre la comercialización de equipos radioeléctricos, y por la que se deroga la Directiva 1999/5/CE.
d) Directiva 2014/30/UE, del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, sobre la armonización de las legislaciones de los Estados miembros en materia de compatibilidad electromagnética.
e) Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).

2. Mediante esta ley se adoptan medidas para la ejecución o aplicación de los siguientes Reglamentos:

a) Reglamento (UE) 531/2012, del Parlamento Europeo y del Consejo, de 13 de junio de 2012, relativo a la itinerancia en las redes públicas de comunicaciones móviles en la Unión.
b) Reglamento (UE) 2015/2120, del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, por el que se establecen medidas en relación con el acceso a una internet abierta y tarifas al por menor para comunicaciones intracomunitarias reguladas y se modifican la Directiva 2002/22/CE y el Reglamento (UE) 531/2012.

Disposición final quinta. *Habilitación para el desarrollo reglamentario.*

Se habilita al Gobierno y a la persona titular del Ministerio de Asuntos Económicos y Transformación Digital, en el ámbito de sus respectivas competencias, para el desarrollo y ejecución de lo dispuesto en esta ley.

Disposición final sexta. *Entrada en vigor.*

1. La presente ley entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado», salvo lo dispuesto en el apartado siguiente.
2. El derecho de los usuarios finales a no recibir llamadas no deseadas con fines de comunicación comercial contemplado en el artículo 66.1.b) entrará en vigor en el plazo de un año a contar desde la publicación de la presente ley en el «Boletín Oficial del Estado». Hasta ese momento, los usuarios finales de los servicios de comunicaciones interpersonales disponibles al público basados en la numeración podrán seguir ejercitando el derecho a oponerse a recibir llamadas no deseadas con fines de comunicación comercial que se efectúen mediante sistemas distintos de los establecidos en el artículo 66.1.a) y a ser informados de este derecho.

ANEXO I

Tasas en materia de telecomunicaciones

1. Tasa general de operadores

1. Hecho imponible. Constituye el hecho imponible de la tasa general de operadores la prestación de servicios y realización de actividades por la Secretaría de Estado de

Telecomunicaciones e Infraestructuras Digitales y por la Comisión Nacional de los Mercados y la Competencia en aplicación del régimen jurídico establecido en esta ley.

2. Sujetos pasivos. Tendrán la consideración de sujetos pasivos de la tasa los operadores inscritos en el Registro general de operadores a que se refiere el artículo 7 obligados a satisfacer la tasa anual de acuerdo con lo establecido en el apartado 6.

3. Base imponible. Constituye la base imponible de la tasa los ingresos brutos de explotación que obtenga el operador obligado derivados del suministro de las redes y la prestación de los servicios de comunicaciones electrónicas incluidos en el ámbito de aplicación de esta ley. A tales efectos, no se considerarán como ingresos brutos los correspondientes a servicios prestados por un operador cuyo importe recaude de los usuarios con el fin de remunerar los servicios de operadores que suministren redes o presten servicios de comunicaciones electrónicas.

4. Tipo impositivo. El tipo impositivo no podrá exceder el 1 por mil de los ingresos brutos de explotación de los operadores obligados al pago.

5. Devengo. La tasa se devengará el 31 de diciembre de cada año. No obstante, si por causa imputable al operador, este perdiera la habilitación para actuar como tal en fecha anterior al 31 de diciembre, la tasa se devengará en la fecha en que esta circunstancia se produzca.

Los operadores de comunicaciones electrónicas obligados a satisfacer la tasa anual de acuerdo con lo establecido en el apartado 6 estarán obligados a presentar una declaración anual de sus ingresos brutos de explotación, en el plazo de seis meses desde la fecha de devengo de la tasa.

6. Obligados al pago de la tasa. Los operadores que obtengan por el suministro de redes o la prestación de servicios de comunicaciones electrónicas unos ingresos brutos de explotación anuales superiores a 1 millón de euros estarán obligados a satisfacer la tasa general de operadores, cuyo importe no podrá exceder el 1 por mil de sus ingresos brutos de explotación, como se señala en el apartado 4.

7. Objeto de la tasa. Los gastos a sufragar son los que se generen, incluidos los de gestión, control y ejecución, por la aplicación del régimen jurídico establecido en esta ley, por las autoridades públicas competentes específicas en materia de telecomunicaciones a que se refiere el artículo 98. En concreto, los gastos a sufragar serán los gastos de personal y gastos corrientes en que incurran la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales y la Comisión Nacional de los Mercados y la Competencia en el ejercicio de sus funciones directamente relacionadas con la aplicación del régimen jurídico establecido en esta ley, y en especial las funciones de regulación, supervisión, resolución de litigios e imposición de sanciones.

8. Mecanismo para el cálculo de la tasa. El importe de esta tasa anual no podrá exceder de los gastos que se generen, incluidos los de gestión, control y ejecución, por la aplicación del régimen jurídico establecido en esta ley, anteriormente referidos.

A tal efecto, la Comisión Nacional de los Mercados y la Competencia hará pública antes del 30 de abril de cada año una memoria que contenga los gastos de personal y gastos corrientes en que han incurrido la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales y la Comisión Nacional de los Mercados y la Competencia en el ejercicio anterior por la aplicación del régimen jurídico establecido en esta ley.

La memoria contemplará, de forma separada, los gastos de personal y gastos corrientes en los que haya incurrido la Comisión Nacional de los Mercados y la Competencia por la aplicación del régimen jurídico establecido en esta ley, que servirán de base para fijar la asignación anual de la Comisión con cargo a los Presupuestos Generales del Estado y garantizar la suficiencia de recursos financieros de la Comisión para la aplicación de esta ley.

El importe de la tasa resultará de aplicar al importe de los gastos en que han incurrido en el ejercicio anterior las autoridades públicas mencionadas que figura en la citada memoria, el porcentaje que individualmente representan los ingresos brutos de explotación de cada uno de los operadores de comunicaciones electrónicas obligados en el ejercicio anterior sobre el total de los ingresos brutos de explotación obtenidos en ese mismo ejercicio por los operadores de comunicaciones electrónicas.

9. Desarrollo reglamentario. Mediante real decreto se determinará el sistema para calcular los gastos de personal y gastos corrientes en que han incurrido la Secretaría de

Estado de Telecomunicaciones e Infraestructuras Digitales y la Comisión Nacional de los Mercados y la Competencia en el ejercicio de sus funciones directamente relacionadas con la aplicación del régimen jurídico establecido en esta ley, el sistema de gestión para la liquidación de esta tasa y los plazos y requisitos que los operadores de comunicaciones electrónicas obligados a satisfacer la tasa anual de acuerdo con lo establecido en el apartado 1 deben cumplir para declarar a la Comisión Nacional de los Mercados y la Competencia el importe de sus ingresos brutos de explotación, con el objeto de que esta calcule el importe de la tasa que corresponde satisfacer a cada uno de los operadores de comunicaciones electrónicas.

Si la referida declaración de ingresos no se presentase en plazo, se formulará al sujeto pasivo requerimiento notificado con carácter fehaciente, a fin de que en el plazo de diez días hábiles presente la declaración. Si no lo hiciera, el órgano gestor le girará una liquidación provisional sobre los ingresos brutos de explotación determinados en régimen de estimación indirecta, conforme a lo dispuesto en el artículo 53 de la Ley 58/2003, de 17 de diciembre, General Tributaria, incluyendo, el importe de la sanción y los intereses de demora que procedan. Respecto de la imposición de la sanción se estará a lo dispuesto en la citada Ley General Tributaria.

2. Tasas por numeración

1. Constituye el hecho imponible de la tasa el otorgamiento de derechos de uso de números. Serán sujetos pasivos de la tasa las personas físicas o jurídicas beneficiarias de derechos de uso.

La tasa se devengará el 1 de enero de cada año, excepto la del período inicial, que se devengará en la fecha que se produzca el otorgamiento de los derechos de uso.

El procedimiento para su exacción se establecerá por real decreto. El importe de dicha exacción será el resultado de multiplicar la cantidad de números cuyos derechos de uso se hayan otorgado por el valor de cada uno de ellos, que podrá ser diferente en función de los servicios y planes correspondientes.

Con carácter general, el valor de cada número del Plan nacional de numeración para la fijación de la tasa por numeración, incluyendo a estos efectos los números empleados exclusivamente para la prestación de servicios de mensajes sobre redes telefónicas, será de 0,041 euros. A este valor se le aplicarán los coeficientes que se especifican en la siguiente tabla, para los rangos y servicios que se indican:

Coeficiente	Servicio	Rango (NXYA)	Longitud (cifras)
0	Servicios de interés social.	0XY, 112, 10YA	3 y 4
0	Servicios armonizados europeos de valor social.	116 A (A = 0 y 1)	6
0	Uso interno en el ámbito de cada operador.	12YA (YA= 00 - 19)	Indefinida
		22YA	
2	Mensajes sobre redes telefónicas.	2XYA (X ≠ 2)	5 y 6
		3XYA	
		79YA	
		99YA	
3	Numeración corta y prefijos.	1XYA (X≠1)	4, 5 y 6
		50YA	
1	Numeración geográfica.	9XYA (X≠0)	9
		8XYA (X≠0)	
1	Numeración móvil.	6XYA	9
		7XYA (X=1, 2, 3, 4)	
1	Numeración nómada no geográfica.	5XYA (X=1)	9
1	Numeración de acceso a internet.	908A	9
		909A	
10	Tarifas especiales.	80YA (Y=0, 3, 6, 7)	9
		90YA (Y=0, 1, 2, 5, 7)	
10	Numeración personal.	70YA	9
30	Consulta telefónica sobre números de abonado.	118 A (A= 1 - 9)	5
2	Comunicaciones máquina a máquina.	590 A	13

Nota: En la columna correspondiente a la identificación de rango, las cifras NXYA representan las primeras 4 cifras del número marcado. Las cifras X, Y, A pueden tomar todos los valores entre 0 y 9, excepto en los casos que se indique otra cosa. El guion indica que las cifras referenciadas pueden tomar cualquier valor comprendido entre los mostrados a cada lado del mismo (estos incluidos).

El Plan nacional de numeración y sus disposiciones de desarrollo podrán introducir coeficientes a aplicar para los recursos de numeración que se atribuyan con posterioridad a

la entrada en vigor de esta ley, siempre que aquellos no sobrepasen el valor de 30, exceptuando los supuestos en que se otorguen derechos de uso de números de 9 cifras a usuarios finales, en cuyo caso el valor máximo resultante de la tasa no podrá superar los 100 euros.

A los efectos del cálculo de esta tasa, se entenderá que todos los números del Plan nacional de numeración, y los empleados exclusivamente para la prestación de servicios de mensajes sobre redes telefónicas públicas, están formados por nueve dígitos. Cuando se otorguen derechos de uso de un número con menos dígitos, se considerará que se están otorgando derechos de uso para la totalidad de los números de nueve dígitos que se puedan formar manteniendo como parte inicial de éstos el número cuyos derechos de uso se otorgan. Cuando se otorguen derechos de uso de números de mayor longitud, se considerará que se están otorgando para la totalidad de los números de nueve dígitos que se puedan formar con las nueve primeras cifras de aquellos.

Asimismo, se establecen las siguientes tasas por numeración:

Tipo de número	Norma de referencia	Valor de cada código (euros)
Código de punto de señalización internacional (CPSI).	Recomendación UIT-T Q.708.	1.000
Código de punto de señalización nacional (CPSN).	Recomendación UIT-T Q.704.	10
Indicativo de red de datos (CIRD).	Recomendación UIT-T X.121.	1.000
Indicativo de red móvil Tetra (IRM).	Recomendación UIT-T E.218.	1.000
Código de operador de portabilidad (NRN).	Especificaciones técnicas de portabilidad.	1.000
Indicativo de red móvil (IRM).	Recomendación UIT-T E.212.	1.000

El valor de la tasa por numeración se fijará anualmente en la Ley de Presupuestos Generales del Estado.

2. No obstante lo dispuesto en el epígrafe anterior, en la fijación del importe a satisfacer por esta tasa se podrá tomar en consideración el valor de mercado del uso de los números cuyos derechos de uso se otorguen y la rentabilidad que de ellos pudiera obtener la persona o entidad beneficiaria, conforme a lo dispuesto en el artículo 30.

En este caso, en los supuestos de carácter excepcional en que así esté previsto en los planes nacionales o sus disposiciones de desarrollo y en los términos que en éstos se fijen, la cuantía anual de la tasa podrá sustituirse por la que resulte de un procedimiento de licitación en el que se fijará un valor inicial de referencia y el tiempo de duración del otorgamiento del derecho de uso. Si el valor de adjudicación de la licitación resultase superior a dicho valor de referencia, aquél constituirá el importe de la tasa.

3. Procederá la devolución del importe de la tasa por numeración que proporcionalmente corresponda, cuando se produzca la cancelación de la asignación de recursos de numeración a petición del interesado, durante el ejercicio anual que corresponda. Para ello, se seguirá el procedimiento establecido mediante real decreto.

4. El importe de los ingresos obtenidos por esta tasa se ingresará en el Tesoro Público y se destinará a la financiación de los gastos que soporte la Administración General del Estado en la gestión, control y ejecución del régimen jurídico establecido en esta ley.

3. Tasa por reserva del dominio público radioeléctrico

> Véase el art. 85 de la Ley 31/2022, de 23 de diciembre, redactada conforme a la corrección de errores publicada en BOE núm. 52, de 2 de marzo de 2023, en cuanto a la forma de calcular la tasa por reserva de dominio público radioeléctrico establecida en este apartado. Ref. BOE-A-2022-22128

1. La reserva para uso privativo o para uso especial por operadores de cualquier frecuencia del dominio público radioeléctrico a favor de una o varias personas o entidades se gravará con una tasa anual, en los términos que se establecen en este apartado.

Para la fijación del importe a satisfacer en concepto de esta tasa por los sujetos obligados, se tendrá en cuenta el valor de mercado del uso de la frecuencia reservada y la rentabilidad que de él pudiera obtener el beneficiario.

Para la determinación del citado valor de mercado y de la posible rentabilidad obtenida por el beneficiario de la reserva se tomarán en consideración, entre otros, los siguientes parámetros:

a) el grado de utilización y congestión de las distintas bandas y en las distintas zonas geográficas;
b) el tipo de servicio para el que se pretende utilizar la reserva y, en particular, si este lleva aparejadas las obligaciones de servicio público recogidas en los artículos 40 y 43;
c) la banda o sub-banda del espectro que se reserve;
d) los equipos y tecnología que se empleen;
e) el valor económico derivado del uso o aprovechamiento del dominio público reservado.

2. El importe a satisfacer en concepto de esta tasa será el resultado de multiplicar la cantidad de unidades de reserva radioeléctrica del dominio público reservado por el valor en euros que se asigne a la unidad. En los territorios insulares, la superficie a aplicar para el cálculo de las unidades radioeléctricas que se utilicen para la determinación de la tasa correspondiente se calculará excluyendo la cobertura no solicitada que se extienda sobre la zona marítima. A los efectos de lo dispuesto en este apartado, se entiende por unidad de reserva radioeléctrica un patrón convencional de medida, referido a la ocupación potencial o real, durante el período de un año, de un ancho de banda de un kilohercio sobre un territorio de un kilómetro cuadrado.

3. La cuantificación de los parámetros anteriores se determinará por la Ley de Presupuestos Generales del Estado. La reducción del parámetro indicado en el párrafo b) del epígrafe 1 de este apartado de la tasa por reserva de dominio público radioeléctrico, que se determinará en la Ley de Presupuestos Generales del Estado, será de hasta el 75 por 100 del valor de dicho coeficiente para las redes y servicios de comunicaciones electrónicas que lleven aparejadas obligaciones de servicio público de los artículos 40 y 43, o para el dominio público destinado a la prestación de servicios públicos en gestión directa o indirecta mediante concesión administrativa.

Asimismo, en la ley a que se refiere el párrafo anterior se fijará:

a) la fórmula para el cálculo del número de unidades de reserva radioeléctrica de los distintos servicios radioeléctricos;
b) los tipos de servicios radioeléctricos;
c) el importe mínimo a ingresar en concepto de tasa por reserva del dominio público radioeléctrico.

4. El pago de la tasa deberá realizarse por el titular de la reserva de dominio público radioeléctrico. Las estaciones meramente receptoras que no dispongan de reserva radioeléctrica estarán excluidas del pago de la tasa. El importe de la exacción será ingresado en el Tesoro Público.

5. El importe de la tasa habrá de ser satisfecho anualmente. Se devengará inicialmente el día del otorgamiento del título habilitante para el uso del demanio y, posteriormente, el día 1 de enero de cada año.

6. El procedimiento de exacción se establecerá mediante real decreto.

Las notificaciones efectuadas para la gestión, liquidación y exacción de la tasa por reserva del dominio público radioeléctrico a los titulares de la reserva podrán practicarse por comparecencia electrónica, en los términos del artículo 43 de la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas.

El impago del importe de la tasa podrá motivar la suspensión o la pérdida del derecho a la ocupación del dominio público radioeléctrico, salvo cuando, en el procedimiento de impugnación en vía administrativa o contencioso-administrativa interpuesto contra la liquidación de la tasa, se hubiese acordado la suspensión del pago.

7. Las Administraciones públicas estarán exentas del pago de esta tasa en los supuestos de reserva de dominio público radioeléctrico para la prestación de servicios obligatorios de interés general que tenga exclusivamente por objeto la seguridad nacional, la defensa nacional, la seguridad pública y las emergencias, así como cualesquiera otros servicios obligatorios de interés general sin contrapartida económica directa o indirecta, como tasas,

precios públicos o privados, ni otros ingresos derivados de dicha prestación, tales como los ingresos en concepto de publicidad. A tal efecto, deberán solicitar, fundamentadamente, dicha exención al Ministerio de Asuntos Económicos y Transformación Digital. Asimismo, no estarán sujetos al pago los enlaces descendentes de comunicación audiovisual por satélite, tanto radiofónica como televisiva.

4. Tasas de telecomunicaciones

1. La gestión precisa para el otorgamiento de determinadas concesiones y autorizaciones, inscripciones registrales, emisión de certificaciones, realización de actuaciones obligatorias de inspección, emisión de dictámenes técnicos y la realización de exámenes darán derecho a la exacción de las tasas compensatorias del coste de los trámites y actuaciones necesarias, con arreglo a lo que se dispone en los párrafos siguientes.

2. Constituye el hecho imponible de la tasa la gestión precisa por la Administración para la expedición de certificaciones registrales; para la expedición de certificaciones de presentación a la administración de las telecomunicaciones del proyecto técnico de infraestructuras comunes de telecomunicaciones, el acta de replanteo, el boletín de instalación y el protocolo de pruebas y, en su caso, el certificado de fin de obra y sus anexos; para la expedición de certificaciones de cumplimiento de especificaciones técnicas de equipos de telecomunicación; la emisión de dictámenes técnicos de evaluación de la conformidad de equipos de telecomunicación; las inscripciones en el registro de empresas instaladoras de telecomunicación; las actuaciones inspectoras o de comprobación técnica que, con carácter obligatorio, vengan establecidas en esta ley o en otras disposiciones con rango legal; la presentación de certificaciones expedidas por técnico competente sustitutivas de dichas actuaciones inspectoras o de comprobación; la tramitación de concesiones demaniales o autorizaciones para el uso privativo del dominio público radioeléctrico; la tramitación de autorizaciones generales o individuales para el uso especial de dicho dominio y la realización de los exámenes de capacitación para operar estaciones de radioaficionado.

3. Serán sujetos pasivos de la tasa, según los supuestos, la persona natural o jurídica que solicite la correspondiente certificación registral; la que solicite la expedición de certificaciones de presentación a la administración de las telecomunicaciones del proyecto técnico de infraestructuras comunes de telecomunicaciones, el acta de replanteo, el boletín de instalación y el protocolo de pruebas y, en su caso, el certificado de fin de obra y sus anexos; la que solicite la emisión de dictámenes técnicos de evaluación de la conformidad de equipos de telecomunicación; la que presente al registro de empresas instaladoras de telecomunicación la correspondiente declaración responsable; aquella a la que proceda practicar las actuaciones inspectoras de carácter obligatorio; la que presente certificaciones expedidas por técnico competente sustitutivas de dichas actuaciones inspectoras o de comprobación de carácter obligatorio; la que solicite la tramitación de concesiones demaniales o autorizaciones para el uso privativo del dominio público radioeléctrico o la tramitación de autorizaciones, generales o individuales, de uso especial del dominio público radioeléctrico; o la que se presente a los exámenes para la obtención del título de operador de estaciones de radioaficionado.

4. La cuantía de la tasa se establecerá en la Ley de Presupuestos Generales del Estado. La tasa se devengará en el momento de la solicitud correspondiente. El rendimiento de la tasa se ingresará en el Tesoro Público. Mediante real decreto se establecerá la forma de liquidación de la tasa.

La realización de pruebas o ensayos para comprobar el cumplimiento de especificaciones técnicas tendrá la consideración de precio público cuando aquellas puedan efectuarse por el interesado, opcionalmente, en centros dependientes de la Administración de cualquier Estado miembro de la Unión Europea, de la Administración española o en centros privados o ajenos a aquellas, cuando dichas pruebas sean solicitadas por el interesado voluntariamente sin que venga obligado a ello por la normativa en vigor.

5. Estarán exentos del pago de la tasa de tramitación de autorizaciones individuales para el uso especial de dominio público radioeléctrico por radioaficionados aquellos solicitantes de dichas autorizaciones que cumplan sesenta y cinco años en el año en que efectúen la solicitud, o que los hayan cumplido con anterioridad, así como los beneficiarios de una

pensión pública o que tengan reconocido un grado de minusvalía igual o superior al 33 por 100.

5. Gestión y recaudación en período voluntario de las tasas

La Comisión Nacional de los Mercados y la Competencia gestionará y recaudará en período voluntario las tasas que se regulan en los apartados 1 y 2 de este anexo, así como las del apartado 4 que se recauden por la prestación de servicios que tenga encomendados la Comisión Nacional de los Mercados y la Competencia en el ámbito de las comunicaciones electrónicas, de acuerdo con lo previsto en esta ley.

Para el resto de supuestos, la gestión en periodo voluntario de las tasas corresponderá al Ministerio de Asuntos Económicos y Transformación Digital.

ANEXO II

Definiciones

1. Abonado: cualquier persona física o jurídica que haya celebrado un contrato con un proveedor de servicios de comunicaciones electrónicas disponibles para el público para la prestación de dichos servicios.

2. Acceso: la puesta a disposición de otra empresa, en condiciones definidas y sobre una base exclusiva o no exclusiva, de recursos o servicios con fines de prestación de servicios de comunicaciones electrónicas, incluyendo cuando se utilicen para el suministro de servicios de la sociedad de información o de servicios de contenidos de radiodifusión; incluye, entre otras cosas, el acceso a elementos de redes y recursos asociados que pueden requerir la conexión de equipos por medios fijos y no fijos (en particular, esto incluye el acceso al bucle local y a recursos y servicios necesarios para facilitar servicios a través del bucle local); el acceso a infraestructuras físicas, como edificios, conductos y mástiles; el acceso a sistemas informáticos pertinentes, incluidos los sistemas de apoyo operativos; el acceso a sistemas de información o bases de datos para prepedidos, suministros, pedidos, solicitudes de mantenimiento y reparación, y facturación; el acceso a la conversión del número de llamada o a sistemas con una funcionalidad equivalente; el acceso a redes fijas y móviles, en particular con fines de itinerancia; el acceso a sistemas de acceso condicional para servicios de televisión digital y el acceso a servicios de redes virtuales.

3. Acreditación en materia de equipos de telecomunicación: declaración por un organismo nacional de acreditación de que un organismo de evaluación de la conformidad cumple los requisitos fijados con arreglo a normas armonizadas y, cuando proceda, otros requisitos adicionales, incluidos los establecidos en los esquemas sectoriales pertinentes, para ejercer actividades específicas de evaluación de la conformidad.

4. Asignación de frecuencias: Autorización administrativa para que una estación radioeléctrica utilice una frecuencia o un canal radioeléctrico determinado en condiciones especificadas.

5. Atribución de frecuencias: la designación de una banda del espectro radioeléctrico para su uso por uno o más tipos de servicios de radiocomunicación, cuando proceda, en las condiciones que se especifiquen.

6. Bucle local o bucle de abonado de la red pública de comunicaciones electrónicas fija: el circuito físico que conecta el punto de terminación de la red a un dispositivo de distribución o instalación equivalente de la red pública de comunicaciones electrónicas fija.

7. Centro de proceso de datos (CPD): estructuras, o grupos de estructuras, dedicado al alojamiento, la interconexión y el funcionamiento centralizados de tecnologías de la información y equipos de red que proporcionan servicios de almacenamiento, procesamiento y transporte de datos junto con todas las instalaciones e infraestructuras para la distribución de energía y control ambiental.

8. Comercialización de equipos de telecomunicación: todo suministro de un equipo para su distribución, consumo o utilización en el mercado de la Unión en el transcurso de una actividad comercial, ya sea a cambio de pago o a título gratuito

9. Comunicación de emergencia: la emitida a través de los servicios de comunicación interpersonal entre un usuario final y el PSAP con el objeto de pedir y recibir ayuda de emergencia de los servicios de emergencia.

10. Comunicaciones intracomunitarias reguladas: cualquier servicio de comunicaciones interpersonales basadas en números que tenga su origen en el Estado miembro del operador nacional del consumidor y que termine en cualquier número fijo o móvil del plan nacional de numeración de otro Estado miembro, y que se cobre total o parcialmente en función del consumo real.

11. Consumidor: cualquier persona física que utilice o solicite un servicio de comunicaciones electrónicas disponible para el público para fines no profesionales, económicos o comerciales.

12. Dirección: cadena o combinación de cifras y símbolos que identifica los puntos de terminación específicos de una conexión y que se utiliza para encaminamiento.

13. Empresa instaladora de telecomunicación: persona física o jurídica que realice la instalación o el mantenimiento de equipos o sistemas de telecomunicación y que ha presentado la declaración responsable al Registro de empresas instaladoras de telecomunicación para el inicio de la actividad o está inscrita en el Registro de empresas instaladoras de telecomunicación.

14. Equipo avanzado de televisión digital: decodificadores para la conexión a televisores o televisores digitales integrados capaces de recibir servicios de televisión digital interactiva.

15. Equipo de telecomunicación: cualquier aparato o instalación fija que se utilice para la transmisión, emisión o recepción a distancia de signos, señales, escritos, imágenes, sonidos o informaciones de cualquier naturaleza por hilo, radioelectricidad, medios ópticos u otros sistemas electromagnéticos.

16. Equipo que presenta un riesgo: equipo que puede afectar negativamente a la salud y la seguridad de las personas en general, a la salud y la seguridad en el trabajo, a la protección de los consumidores, al medio ambiente, a la seguridad pública o a otros intereses públicos protegidos por la legislación de armonización de la Unión aplicable, en un grado que vaya más allá de lo que se considere razonable y aceptable en relación con su finalidad prevista o en las condiciones de uso normales o razonablemente previsibles del equipo en cuestión, incluida la duración de su utilización y, en su caso, los requisitos de su puesta en servicio, instalación y mantenimiento.

17. Equipo que presenta un riesgo grave: un equipo que presenta un riesgo para el que, sobre la base de una evaluación del riesgo y teniendo en cuenta el uso normal y previsible del equipo, se considere que la combinación de la probabilidad de que se produzca un peligro que cause un daño o perjuicio y su gravedad requiera una rápida intervención de las autoridades de vigilancia del mercado, incluidos los casos en que el riesgo no tenga efectos inmediatos.

18. Equipo radioeléctrico: cualquier aparato de telecomunicación que emite o recibe intencionadamente ondas radioeléctricas para fines de radiocomunicación o radiodeterminación, o el producto eléctrico o electrónico que debe ser completado con un accesorio, como una antena, para emitir o recibir intencionadamente ondas radioeléctricas para fines de radiocomunicación o radiodeterminación.

19. Equipo terminal: el equipo conectado directa o indirectamente a la interfaz de una red pública de telecomunicaciones para transmitir, procesar o recibir información. En ambos casos (conexión directa o indirecta), la conexión podrá realizarse por cable, fibra óptica o vía electromagnética. La conexión será indirecta si se interpone un aparato entre el equipo terminal y la interfaz de la red pública. También se considerarán como equipos terminales los equipos de las estaciones terrenas de comunicación por satélite.

20. Especificación técnica: la especificación que figura en un documento que define las características necesarias de un producto, tales como los niveles de calidad o las propiedades de su uso, la seguridad, las dimensiones, los símbolos, las pruebas y los métodos de prueba, el empaquetado, el marcado y el etiquetado. Se incluyen dentro de la citada categoría las normas aplicables al producto en lo que se refiere a la terminología.

21. Espectro radioeléctrico: ondas electromagnéticas, cuya frecuencia se fija convencionalmente por debajo de 3.000 GHz, que se propagan por el espacio sin guía artificial.

22. Espectro radioeléctrico armonizado: el espectro radioeléctrico cuyas condiciones de disponibilidad y uso eficiente se han armonizado a través de una medida técnica de aplicación de conformidad con el artículo 4 de la Decisión 676/2002/CE.

23. Evaluación de la conformidad: proceso por el que se evalúa si un equipo de telecomunicación satisface los requisitos esenciales aplicables.

24. Incidente de seguridad: un hecho que tenga efectos adversos reales en la seguridad de las redes o servicios de comunicaciones electrónicas.

25. Infraestructura física: cualquier elemento de una red pensado para albergar otros elementos de una red sin llegar a ser un elemento activo de ella, como tuberías, mástiles, conductos, cámaras de acceso, bocas de inspección, distribuidores, edificios o entradas a edificios, instalaciones de antenas, torres y postes. Los cables, incluida la fibra oscura, así como los elementos de redes utilizados para el transporte de agua destinada al consumo humano, no son infraestructura física.

26. Información sobre la localización del llamante: en una red pública de telefonía móvil, los datos procesados, procedentes tanto de la infraestructura de la red como del terminal, que indican la posición geográfica del equipo terminal móvil de un usuario final y, en una red pública de telefonía fija, los datos sobre la dirección física del punto de terminación de la red.

27. Interconexión: un tipo particular de acceso entre operadores de redes públicas mediante la conexión física y lógica de las redes públicas de comunicaciones electrónicas utilizadas por una misma empresa o por otra distinta, de manera que los usuarios de una empresa puedan comunicarse con los usuarios de la misma empresa o de otra distinta, o acceder a los servicios prestados por otra empresa, donde dichos servicios se prestan por las partes interesadas o por terceros que tengan acceso a la red.

28. Interfaz de programa de aplicación (API): la interfaz de software entre las aplicaciones externas, puesta a disposición por los radiodifusores o proveedores de servicios, y los recursos del equipo avanzado de televisión digital para los servicios de radio y televisión digital.

29. Interfaz en línea: todo programa informático, incluidos los sitios web, partes de sitios web o aplicaciones, explotado por un operador económico en materia de equipos de telecomunicación o en su nombre, y que sirve para proporcionar a los consumidores acceso a los productos de dicho operador económico.

30. Interfaz radioeléctrica: Especificación del uso regulado del espectro radioeléctrico.

31. Interferencia perjudicial: una interferencia que suponga un riesgo para el funcionamiento de un servicio de radionavegación o de otros servicios de seguridad o que degrade gravemente, obstruya o interrumpa reiteradamente un servicio de radiocomunicación que funcione de conformidad con la normativa internacional, de la Unión Europea o nacional aplicable.

32. Introducción en el mercado de un equipo de telecomunicación: primera comercialización de un equipo en el mercado de la Unión Europea.

33. Itinerancia en la Unión Europea: el uso por un cliente itinerante de un dispositivo móvil para efectuar o recibir llamadas dentro de la Unión, o para enviar o recibir mensajes SMS dentro de la Unión o para usar comunicaciones de datos por conmutación de paquetes, cuando se encuentra en un Estado miembro distinto de aquel en que está ubicada la red del proveedor nacional, en virtud de acuerdos celebrados entre el operador de la red de origen y el operador de la red visitada.

34. Legislación de armonización de la Unión Europea en materia de equipos de telecomunicación: toda legislación de la Unión Europea que armonice las condiciones para la comercialización de los productos en su territorio.

35. Llamada: una conexión establecida por medio de un servicio de comunicaciones interpersonales disponible para el público que permita la comunicación de voz bidireccional.

36. Mercados transnacionales: los mercados que abarcan toda la Unión Europea o una parte importante de la misma situada en más de un Estado miembro.

37. Microempresa: empresa definida en los términos establecidos en el artículo 2 del anexo I del Reglamento (UE) n.º 651/2014 de la Comisión, de 17 de junio de 2014, por el que se declaran determinadas categorías de ayudas compatibles con el mercado interior en aplicación de los artículos 107 y 108 del Tratado.

38. Pequeña empresa: empresa definida en los términos establecidos en el artículo 2 del anexo I del Reglamento (UE) n.º 651/2014 de la Comisión, de 17 de junio de 2014, por el que se declaran determinadas categorías de ayudas compatibles con el mercado interior en aplicación de los artículos 107 y 108 del Tratado.

39. Nombre: combinación de caracteres (cifras decimales, letras o símbolos) que se utiliza para identificar abonados, usuarios u otras entidades tales como elementos de red.

40. Número: cadena de cifras decimales que, entre otros, pueden representar un nombre o una dirección.

41. Número geográfico: el número identificado en un plan nacional de numeración que contiene en parte de su estructura un significado geográfico utilizado para el encaminamiento de las llamadas hacia la ubicación física del punto de terminación de la red.

42. Número no geográfico: el número identificado en un plan nacional de numeración que no sea número geográfico, tales como los números de teléfonos móviles, los de llamada gratuita y los de tarificación adicional.

43. Obras civiles: cada uno de los resultados de las obras de construcción o de ingeniería civil tomadas en conjunto que se basta para desempeñar una función económica o técnica e implica uno o más elementos de una infraestructura física.

44. Ondas radioeléctricas: Ondas electromagnéticas, cuya frecuencia se fija convencionalmente por debajo de 3.000 GHz, que se propagan por el espacio sin guía artificial.

45. Operador: persona física o jurídica que suministra redes públicas de comunicaciones electrónicas o presta servicios de comunicaciones electrónicas disponibles al público y ha notificado al Registro de operadores el inicio de su actividad o está inscrita en el Registro de operadores.

46. Operador con peso significativo en el mercado: operador que, individual o conjuntamente con otros, disfruta de una posición equivalente a una posición dominante, esto es, una posición de fuerza económica que permite que su comportamiento sea, en medida apreciable, independiente de los competidores, los clientes y, en última instancia, los consumidores.

47. Operador económico en materia de equipos de telecomunicación: el fabricante, el representante autorizado, el importador, el distribuidor, el prestador de servicios logísticos o cualquier otra persona física o jurídica sujeta a obligaciones en relación con la fabricación de productos, su comercialización o su puesta en servicio de conformidad con la legislación de armonización de la Unión Europea aplicable.

a) Distribuidor: toda persona física o jurídica de la cadena de suministro distinta del fabricante o el importador que comercializa un producto.

b) Fabricante: toda persona física o jurídica que fabrica un producto, o que manda diseñar o fabricar un producto y lo comercializa con su nombre o marca.

c) Importador: toda persona física o jurídica establecida en la Unión Europea que introduce un producto de un tercer país en el mercado de la Unión.

d) Prestador de servicios logísticos: toda persona física o jurídica que ofrezca, en el curso de su actividad comercial, al menos dos de los siguientes servicios: almacenar, embalar, dirigir y despachar, sin tener la propiedad de los productos en cuestión y excluidos los servicios postales tal como se definen en el artículo 2, apartado 1, de la Directiva 97/67/CE del Parlamento Europeo y del Consejo, servicios de paquetería, tal como se definen en el artículo 2, apartado 2, del Reglamento UE) 2018/644 del Parlamento Europeo y del Consejo, y cualquier otro servicio postal o servicio de transporte de mercancías

e) Representante autorizado: toda persona física o jurídica establecida en la Unión Europea que ha recibido un mandato por escrito de un fabricante para actuar en su nombre en relación con tareas específicas relativas a obligaciones del fabricante conforme a la legislación aplicable.

48. Organismo de evaluación de la conformidad: organismo que desempeña actividades de evaluación de la conformidad.

49. Organismo nacional de acreditación en materia de equipos de telecomunicación: único organismo de un Estado miembro de la Unión Europea, designado de acuerdo a lo establecido en el Reglamento (UE) 765/2008, del Parlamento y del Consejo, de 9 de julio de

2008, por el que se establecen los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos y por el que se deroga el Reglamento (CEE) n.º 339/93, con potestad pública para llevar a cabo acreditaciones.

50. Organismo notificado: organismo de evaluación de la conformidad notificado a la Comisión Europea y a los demás Estados miembros, por las Autoridades Notificantes.

51. Puesta en servicio de un equipo de telecomunicación: primera utilización del equipo por parte del usuario final.

52. Punto de acceso inalámbrico para pequeñas áreas: un equipo de acceso a una red inalámbrica de baja potencia con un tamaño reducido y corto alcance, utilizando un espectro bajo licencia o una combinación de espectro bajo licencia y exento de licencia que puede formar parte de una red pública de comunicaciones electrónicas, que puede estar dotado de una o más antenas de bajo impacto visual, y que permite el acceso inalámbrico de los usuarios a redes de comunicaciones electrónicas con independencia de la topología de la red subyacente, sea móvil o fija.

53. Punto de intercambio de internet (IXP, por sus siglas en inglés de *Internet Exchange Point*): una instalación de la red que permite interconectar más de dos sistemas autónomos independientes, principalmente para facilitar el intercambio de tráfico de internet; un IXP solo permite interconectar sistemas autónomos; un IXP no requiere que el tráfico de Internet que pasa entre cualquier par de sistemas autónomos participantes pase por un tercer sistema autónomo, ni modifica ni interfiere de otra forma en dicho tráfico.

54. Punto de respuesta de seguridad pública (PSAP): ubicación física en la que se reciben inicialmente las comunicaciones de emergencia y que está bajo la responsabilidad de una autoridad pública o de una organización privada reconocida por el Estado miembro.

55. Punto de terminación de la red: el punto físico en el que el usuario final accede a una red pública de comunicaciones electrónicas. Cuando se trate de redes en las que se produzcan operaciones de conmutación o encaminamiento, el punto de terminación de la red estará identificado mediante una dirección de red específica, la cual podrá estar vinculada a un número o a un nombre de usuario final.

56. Radiocomunicación: toda telecomunicación transmitida por medio de ondas radioeléctricas.

57. Radiodeterminación: Determinación de la posición, velocidad u otras características de un objeto, u obtención de información relativa a estos parámetros, mediante las propiedades de propagación de las ondas radioeléctricas.

58. Recuperación de un equipo de telecomunicación: Cualquier medida destinada a obtener la devolución de un equipo que ya haya sido puesto a disposición del usuario final.

59. Recursos asociados: los servicios asociados, las infraestructuras físicas y otros recursos o elementos asociados con una red de comunicaciones electrónicas o con un servicio de comunicaciones electrónicas que permitan o apoyen el suministro de servicios a través de dicha red o servicio o tengan potencial para ello, e incluyan edificios o entradas de edificios, el cableado de edificios, antenas, torres y otras construcciones de soporte, conductos, mástiles, bocas de acceso y distribuidores.

60. Red de área local radioeléctrica (RLAN): sistema de acceso inalámbrico de baja potencia y corto alcance, con bajo riesgo de interferencia con otros sistemas del mismo tipo desplegados por otros usuarios en las proximidades, que utiliza de forma no exclusiva un espectro radioeléctrico armonizado.

61. Red de comunicaciones electrónicas: los sistemas de transmisión, se basen o no en una infraestructura permanente o en una capacidad de administración centralizada, y, cuando proceda, los equipos de conmutación o encaminamiento y demás recursos, incluidos los elementos de red que no son activos, que permitan el transporte de señales mediante cables, ondas hertzianas, medios ópticos u otros medios electromagnéticos con inclusión de las redes de satélites, redes fijas (de conmutación de circuitos y de paquetes, incluido internet) y móviles, sistemas de tendido eléctrico, en la medida en que se utilicen para la transmisión de señales, redes utilizadas para la radiodifusión sonora y televisiva y redes de televisión por cable, con independencia del tipo de información transportada.

62. Red de comunicaciones electrónicas de alta capacidad: red de comunicaciones electrónicas capaz de prestar servicios de acceso de banda ancha a velocidades de al menos 30 Mbps.

63. Red de comunicaciones electrónicas de muy alta capacidad: bien una red de comunicaciones electrónicas que se compone totalmente de elementos de fibra óptica, al menos hasta el punto de distribución de la localización donde se presta el servicio o una red de comunicaciones electrónicas capaz de ofrecer un rendimiento de red similar en condiciones usuales de máxima demanda, en términos de ancho de banda disponible para los enlaces ascendente y descendente, resiliencia, parámetros relacionados con los errores, latencia y su variación. El rendimiento de la red puede considerarse similar independientemente de si la experiencia del usuario final varía debido a las características intrínsecamente diferentes del medio a través del cual, en última instancia, la red se conecta al punto de terminación de la red.

64. Red pública de comunicaciones electrónicas: una red de comunicaciones electrónicas que se utiliza, en su totalidad o principalmente, para la prestación de servicios de comunicaciones electrónicas disponibles para el público y que soporta la transferencia de información entre puntos de terminación de la red.

65. Reserva de frecuencias: Porción de espectro radioeléctrico cuyos derechos de uso se otorgan por la Administración a una persona física o jurídica en condiciones especificadas.

66. Retirada de un equipo de telecomunicación: Cualquier medida destinada a impedir la comercialización de un equipo que se encuentra en la cadena de suministro.

67. Seguridad de las redes o servicios: la capacidad de las redes y servicios de comunicaciones electrónicas de resistir, con un determinado nivel de confianza, cualquier acción que comprometa la disponibilidad, autenticidad, integridad y confidencialidad de dichas redes y servicios, de los datos almacenados, procesados o transmitidos y la seguridad de los servicios conexos que dichas redes y servicios de comunicaciones electrónicas ofrecen o hacen accesibles.

68. Servicios asociados: aquellos servicios asociados con una red de comunicaciones electrónicas o con un servicio de comunicaciones electrónicas que permitan o apoyen el suministro, la autoprestación o la prestación de servicios automatizada a través de dicha red o servicio o tengan potencial para ello e incluyen la traducción de números o sistemas con una funcionalidad equivalente, los sistemas de acceso condicional y las guías electrónicas de programas, así como otros servicios tales como el servicio de identidad, localización y presencia.

69. Servicio de acceso a internet: servicio de comunicaciones electrónicas a disposición del público que proporciona acceso a internet y, por ende, conectividad entre prácticamente todos los puntos extremos conectados a internet, con independencia de la tecnología de red y del equipo terminal utilizados.

70. Servicio de comunicaciones electrónicas: el prestado por lo general a cambio de una remuneración a través de redes de comunicaciones electrónicas, que incluye, con la excepción de los servicios que suministren contenidos transmitidos mediante redes y servicios de comunicaciones electrónicas o ejerzan control editorial sobre ellos, los siguientes tipos de servicios:

a) el servicio de acceso a internet

b) el servicio de comunicaciones interpersonales, y

c) servicios consistentes, en su totalidad o principalmente, en el transporte de señales, como son los servicios de transmisión utilizados para la prestación de servicios máquina a máquina y para la radiodifusión.

71. Servicio de comunicaciones interpersonales: el prestado por lo general a cambio de una remuneración que permite un intercambio de información directo, interpersonal e interactivo a través de redes de comunicaciones electrónicas entre un número finito de personas, en el que el iniciador de la comunicación o participante en ella determina el receptor o receptores y no incluye servicios que permiten la comunicación interpersonal e interactiva como una mera posibilidad secundaria que va intrínsecamente unida a otro servicio.

72. Servicio de comunicaciones interpersonales basados en numeración: servicio de comunicaciones interpersonales que bien conecta o permite comunicaciones con recursos de numeración pública asignados, es decir, de un número o números de los planes de

numeración nacional o internacional, o permite la comunicación con un número o números de los planes de numeración nacional o internacional.

73. Servicio de comunicaciones interpersonales independiente de la numeración: servicio de comunicaciones interpersonales que no conecta a través de recursos de numeración pública asignados, es decir, de un número o números de los planes de numeración nacional o internacional, o no permite la comunicación con un número o números de los planes de numeración nacional o internacional.

74. Servicio de comunicaciones vocales: un servicio de comunicaciones electrónicas disponible para el público a través de uno o más números de un plan nacional o internacional de numeración telefónica, para efectuar y recibir, directa o indirectamente, llamadas nacionales o nacionales e internacionales.

75. Servicios de conversación total: un servicio de conversación multimedia en tiempo real que proporciona transferencia bidireccional simétrica en tiempo real de vídeo en movimiento, texto en tiempo real y voz entre usuarios de dos o más ubicaciones.

76. Servicio de emergencia: un servicio mediante el que se proporciona asistencia rápida e inmediata en situaciones en que exista, en particular, un riesgo directo para la vida o la integridad física de las personas, para la salud y seguridad públicas o individuales, o para la propiedad pública o privada o el medio ambiente, de conformidad con la normativa nacional.

77. Sistema de acceso condicional: toda medida técnica, sistema de autenticación o mecanismo técnico que condicione el acceso en forma inteligible a un servicio protegido de radiodifusión sonora o televisiva al pago de una cuota u otra forma de autorización individual previa.

78. Suministro de una red de comunicación electrónica: la instalación, la explotación, el control o la puesta a disposición de dicha red.

79. Telecomunicaciones: toda transmisión, emisión o recepción de signos, señales, escritos, imágenes, sonidos o informaciones de cualquier naturaleza por hilo, radioelectricidad, medios ópticos u otros sistemas electromagnéticos.

80. Teléfono público de pago: un teléfono accesible al público en general y para cuya utilización pueden emplearse como medios de pago monedas, tarjetas de crédito/débito o tarjetas de prepago, incluidas las tarjetas que utilizan códigos de marcación.

81. Uso compartido del dominio radioeléctrico: el acceso por parte de dos o más usuarios a las mismas bandas del espectro radioeléctrico con arreglo a un sistema determinado de uso compartido, incluidos los enfoques reguladores tales como el acceso compartido bajo título habilitante tendentes a facilitar el uso compartido de una banda del espectro radioeléctrico, sobre la base de un acuerdo vinculante para todas las partes interesadas y con arreglo a normas de uso compartido vinculadas a los derechos de uso del espectro radioeléctrico, a fin de garantizar a todos los usuarios unas condiciones fiables y previsibles, y sin perjuicio de la aplicación del Derecho de la competencia.

82. Usuario: una persona física o jurídica que utiliza o solicita un servicio de comunicaciones electrónicas disponible para el público.

83. Usuario final: el usuario que no suministra redes públicas de comunicaciones electrónicas o servicios de comunicaciones electrónicas disponibles para el público, ni tampoco los comercializa.

ANEXO III

Conjunto mínimo de los servicios que deberá soportar el servicio de acceso adecuado a internet de banda ancha a que se refiere el artículo 37.1.a):

1.º) correo electrónico;

2.º) motores de búsqueda que permitan la búsqueda y obtención de información de todo tipo;

3.º) herramientas básicas de formación y educación en línea;

4.º) prensa o noticias en línea;

5.º) adquisición o encargo de bienes o servicios en línea;

6.º) búsqueda de empleo y herramientas para la búsqueda de empleo;

7.º) establecimiento de redes profesionales;

8.º) banca por internet;

9.º) utilización de servicios de administración electrónica;
10.º) redes sociales y mensajería instantánea;
11.º) llamadas telefónicas y videollamadas (calidad estándar).

§ 41

Real Decreto 123/2017, de 24 de febrero, por el que se aprueba el Reglamento sobre el uso del dominio público radioeléctrico

Ministerio de Energía, Turismo y Agenda Digital
«BOE» núm. 57, de 8 de marzo de 2017
Última modificación: 18 de enero de 2023
Referencia: BOE-A-2017-2460

La Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, ha introducido importantes novedades en el régimen jurídico de las telecomunicaciones, que van dirigidas a poner en práctica reformas estructurales en el sector de las telecomunicaciones, principalmente enfocadas a que los operadores tengan más facilidad en el despliegue de sus redes y en la prestación de sus servicios, lo cual, en última instancia, redundará en una oferta de servicios a los ciudadanos cada vez con mayor cobertura, más innovadores y de mayor calidad, y en unas mejores condiciones de competitividad y productividad de la economía española.

Estas modificaciones en el régimen jurídico de las telecomunicaciones introducidas por la Ley General de Telecomunicaciones resultan de especial incidencia en la planificación, gestión y control del dominio público radioeléctrico.

Asimismo, la Agenda Digital española, aprobada por el Gobierno el 15 de febrero de 2013, incorpora a nivel nacional los objetivos de la Agenda Digital para Europa, entre ellos el de facilitar en 2020 a todos los ciudadanos accesos de banda ancha con velocidades mínimas de 30 Mbps.

La Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, constituye la norma básica que desarrolla a nivel nacional los objetivos de la Agenda Digital estableciendo un marco legal armonizado que facilite el desarrollo de las infraestructuras de las telecomunicaciones y la puesta a disposición de los ciudadanos de servicios de calidad a precios competitivos.

En la consecución de estos objetivos, el espectro radioeléctrico, como soporte de las radiocomunicaciones, tanto para aplicaciones fijas como, y especialmente, de banda ancha en movilidad, constituye un recurso cada día más estratégico, valioso y demandado, que precisa de una regulación que compatibilice un acceso más flexible al mismo por parte de operadores y usuarios en general, con un aprovechamiento efectivo y con máxima eficiencia.

La Ley 9/2014, de 9 de mayo General de Telecomunicaciones, dedica su título V a la regulación del espectro radioeléctrico, declarándolo bien de dominio público, cuya titularidad y administración corresponden al Estado. La ley recoge los principios aplicables a la administración del espectro radioeléctrico y las actuaciones que abarca dicha administración, clarifica los diferentes usos y los correspondientes títulos habilitantes para el uso del dominio público radioeléctrico. Asimismo, introduce una simplificación administrativa para el acceso a determinadas bandas de frecuencias y consolida las últimas reformas en materia de duración, modificación, extinción y revocación de títulos y en relación al mercado secundario

del espectro y la transferencia de los títulos habilitantes para el uso del dominio público radioeléctrico. Además, la ley introduce medidas destinadas a evitar el uso del espectro por quienes no disponen de autorización para ello, obtenida tras las correspondientes autorizaciones administrativas para la aprobación del proyecto técnico y el reconocimiento satisfactorio de las instalaciones, garantizando así la disponibilidad y uso eficiente de este recurso escaso. Por todo ello, resulta oportuna y necesaria la aprobación de un nuevo Reglamento regulador del dominio público radioeléctrico.

Este nuevo reglamento desarrolla los principios y objetivos que deben inspirar la planificación, administración y control del dominio público radioeléctrico y establece las diferentes actuaciones que abarcan dichas facultades.

Los principios de neutralidad tecnológica y de servicios se ven ampliamente reforzados al establecer como principio general, salvo excepciones tasadas, la posibilidad de uso de cualquier banda de frecuencias para cualquier servicio de radiocomunicaciones y con cualquier tecnología, flexibilizando al máximo su explotación.

También se clarifican los diferentes tipos de uso (común, especial o privativo) y los distintos títulos habilitantes para el uso del dominio público radioeléctrico necesarios para cada uno de dichos usos, introduciendo, por ejemplo, la figura de la autorización general para el uso especial, que habilita a su titular para el uso compartido, sin limitación de número de operadores o usuarios de determinadas bandas de frecuencias, siendo suficiente para su obtención una mera notificación.

En cuanto al otorgamiento de títulos habilitantes para el uso privativo de recursos órbita-espectro, se introduce la posibilidad de otorgar, con determinadas limitaciones, una autorización provisional, condicionada al resultado de las coordinaciones internacionales de frecuencias y del reconocimiento de la reserva por la Unión Internacional de Telecomunicaciones.

El reglamento normaliza los diferentes trámites administrativos en función del tipo de estación, tanto en la parte correspondiente a la aprobación del proyecto técnico y la correspondiente autorización para realizar la instalación, como en la autorización para la puesta en servicio, si bien en la línea de reducción de cargas administrativas instaurada por la nueva Ley General de Telecomunicaciones, el presente reglamento exige menos trámites administrativos y simplifica las obligaciones de información de los operadores.

En este ámbito el reglamento introduce, como novedades importantes, la posibilidad de que tanto en el procedimiento de aprobación del proyecto técnico y la correspondiente autorización para la instalación de determinados tipos de estaciones radioeléctricas, como en el procedimiento de autorización para la puesta en servicio, se pueda realizar a través de procedimientos simplificados, introduciendo la figura del proyecto técnico tipo o de características técnicas tipo para estaciones con características técnicas similares y casos de despliegues masivos de estaciones. Igualmente se simplifican determinados procedimientos reforzando la presentación de declaraciones responsables y certificaciones de que la instalación cumple con los parámetros técnicos aplicables, en sustitución del acto de reconocimiento técnico de las instalaciones por la administración.

En el ámbito de los servicios de telecomunicaciones para la defensa nacional y, en definitiva, de las redes, servicios, instalaciones y equipos de telecomunicaciones que desarrollen actividades esenciales para la defensa nacional y que integren los medios destinados a ésta, la ley establece que se regirán por su normativa específica. Con este fin se incluye un nuevo título en el presente reglamento en desarrollo de los artículos 4.2 y 4.3 de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones que, además de reducir los trámites administrativos, tiene en cuenta la singularidad de estos servicios y la confidencialidad o la urgencia, que, en determinados casos, puede estar asociada a los mismos y que hace que tengan un tratamiento especial.

En el apartado de mercado secundario del espectro, se contemplan cuatro tipos de negocios jurídicos, la transferencia de títulos habilitantes de uso privativo del espectro, cesión y mutualización de derechos de uso privativo, y la provisión de servicios mayoristas relevantes. El reglamento clarifica y simplifica el procedimiento de autorización, haciendo extensiva la posibilidad de transferencia a cualquier título, sin más limitaciones que las establecidas en la presente norma. Asimismo se precisan determinadas medidas contra

comportamientos especulativos o acaparamiento de derechos de uso del dominio público radioeléctrico.

Se efectúa una reordenación más racional en lo relativo a la duración, modificación, extinción y revocación de los títulos habilitantes para el uso del dominio público radioeléctrico, regulando todos estos aspectos en un solo título. En cuanto a la renovación de los títulos, desaparece el requisito de solicitud previa del interesado, siendo la Administración quien comunique de oficio las opciones posibles en cuanto a su continuidad.

Se incluye un título nuevo destinado la inspección y control del dominio público radioeléctrico donde se definen las facultades de la inspección y otro donde se define el procedimiento para ejercitar la potestad de la protección activa del espectro frente a ocupaciones por quienes no disponen de título habilitante preceptivo para el uso del dominio público radioeléctrico.

Igualmente, en conformidad con lo establecido en el apartado b del artículo 61 de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, se incorpora a este reglamento el procedimiento de control e inspección de los niveles únicos de emisión radioeléctrica tolerable y que no supongan un peligro para la salud pública, con la correspondiente actualización tecnológica de los servicios radioeléctricos, así como un título relativo a la protección del dominio público radioeléctrico, que incluye la normativa sobre establecimiento de limitaciones y servidumbres, hasta ahora incluidos dentro del Real Decreto 1066/2001, de 28 de septiembre, por el que se aprueba el Reglamento que establece condiciones de protección del dominio público radioeléctrico, restricciones a las emisiones radioeléctricas y medidas de protección sanitaria frente a emisiones radioeléctricas que, tras esta modificación, regulará exclusivamente las medidas de protección sanitaria frente a emisiones radioeléctricas. Asimismo, se incluye en este título un capítulo dedicado a la nueva figura de la protección activa del espectro.

Con el objetivo de generalizar el uso de las nuevas tecnologías y los nuevos servicios de telecomunicación y de convertir a la Administración Pública en impulsora del proceso de modernización de toda la sociedad, los apartados 2 y 3 del artículo 14 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, permiten establecer reglamentariamente la obligatoriedad de comunicarse con la Administración utilizando únicamente medios electrónicos cuando los interesados, por razón de su capacidad económica o técnica, dedicación profesional u otros motivos acreditados, tengan garantizado el acceso y disponibilidad de los medios tecnológicos precisos. La Orden IET/1902/2012, de 6 de septiembre, por la que se crea y regula el Registro Electrónico del Ministerio de Industria, Energía y Turismo ya estableció la obligatoriedad de comunicación con la Administración únicamente por medios electrónicos para las personas jurídicas.

Con el fin de continuar el impulso y dinamización de la actividad en general, se extiende a todos los interesados, salvo que específicamente se indique lo contrario, la obligatoriedad de comunicarse únicamente por medios electrónicos con la Administración, puesto que la propia naturaleza de lo solicitado conlleva necesariamente la disposición de unas capacidades técnicas o económicas mínimas.

Este real decreto consta de un artículo único que aprueba el reglamento, tres disposiciones adicionales, cinco disposiciones transitorias; una disposición derogatoria y cuatro disposiciones finales. La disposición adicional primera versa sobre la presentación de documentos por medios electrónicos, la segunda sobre la continuidad de los datos del registro público de concesiones, y la tercera sobre el control del gasto público. Las tres primeras disposiciones transitorias se refieren a los procedimientos iniciados con anterioridad a su entrada en vigor, a las solicitudes de autorización para la puesta en servicio de estaciones con autorización para la instalación a su entrada en vigor, y a la utilización de modelos aprobados conforme a la normativa anterior. La disposición transitoria cuarta se refiere a la continuidad de las condiciones asociadas a los títulos otorgados con anterioridad. La disposición transitoria quinta se refiere a los negocios jurídicos formalizados con anterioridad a la entrada en vigor de este reglamento.

La disposición final primera modifica la Orden CTE/23/2002, de 11 de enero, por la que se establecen condiciones para la presentación de determinados estudios y certificaciones por operadores de servicios de radiocomunicaciones, al objeto de completar la definición de las diferentes tipologías de estaciones y precisar los conceptos relativos a la ubicación de

estaciones en suelo urbano y donde permanezcan habitualmente personas. El resto de las disposiciones finales corresponden a las facultades de desarrollo, el título competencial y la entrada en vigor.

El reglamento que se aprueba incluye dos disposiciones adicionales, la primera de las cuales identifica las bandas de frecuencias con limitación de títulos habilitantes para el uso del dominio público radioeléctrico a otorgar; así como dos anexos, el primero de ellos especifica los servicios con frecuencias reservadas en las bandas susceptibles de cesión a terceros de los derechos de uso del dominio público radioeléctrico, y el anexo 2 establece limitaciones y servidumbres para la protección de determinadas instalaciones radioeléctricas.

Durante su tramitación el real decreto ha sido objeto de informe por la Comisión Nacional de los Mercados y la Competencia y por el Consejo Asesor de las Telecomunicaciones y de la Sociedad de la Información. De conformidad con lo establecido en la disposición adicional quinta de la Ley General de Telecomunicaciones, el informe de este último órgano equivale a la audiencia a la que se refiere el artículo 24 de la Ley 50/1997, de 27 de noviembre, del Gobierno.

En su virtud, a propuesta del Ministro de Energía, Turismo y Agenda Digital, con la aprobación previa del Ministro de Hacienda y Función Pública, de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros en su reunión del día 24 de febrero de 2017,

DISPONGO:

Artículo único. *Aprobación del reglamento.*

Se aprueba el Reglamento sobre el uso del dominio público radioeléctrico, que se inserta a continuación.

Disposición adicional primera. *Tramitación en sede electrónica de los procedimientos administrativos derivados de este real decreto.*

La tramitación de los procedimientos contemplados en el reglamento que se aprueba por este real decreto, así como la relación con los órganos competentes del Ministerio de Energía, Turismo y Agenda Digital sobre los aspectos contemplados en el mismo, se deberá llevar a cabo obligatoriamente por medios electrónicos en el plazo de seis meses desde su entrada en vigor, siempre que estén disponibles en la sede electrónica de dicho Ministerio.

Cuando en un procedimiento concreto se establezcan modelos específicos de presentación de solicitudes en la sede electrónica del Ministerio, los interesados deberán utilizar estos modelos.

Disposición adicional segunda. *Registro público de concesiones.*

A la entrada en vigor del presente real decreto y del reglamento que aprueba, los datos que figuren en el Registro público de concesionarios del artículo 8 del Reglamento de desarrollo de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, en lo relativo al uso del dominio público radioeléctrico se traspasarán, de oficio, al Registro público de concesiones regulado en el artículo 9 del reglamento aprobado por el presente real decreto.

Disposición adicional tercera. *Control del gasto público.*

Las medidas incluidas en esta norma no podrán suponer incremento de dotaciones ni de retribuciones ni de otros gastos de personal.

Disposición transitoria primera. *Procedimientos iniciados con anterioridad a la entrada en vigor de este real decreto.*

1. Los procedimientos iniciados con anterioridad a la entrada en vigor del presente real decreto, y del reglamento que aprueba, se tramitarán y resolverán por la normativa vigente en el momento de iniciarse el procedimiento.

2. No obstante lo anterior, el interesado podrá con anterioridad a la resolución desistir de su solicitud y, de este modo, optar por la aplicación del presente real decreto y del reglamento que aprueba.

Disposición transitoria segunda. *Solicitud de autorización para la puesta en servicio de estaciones que dispongan de aprobación del proyecto técnico y la correspondiente autorización para realizar la instalación a la entrada en vigor de este real decreto.*

1. Las estaciones correspondientes a redes y servicios distintos de los mencionados en el apartado 1 del artículo 53 del reglamento que se aprueba mediante este real decreto, que dispongan de la aprobación del proyecto técnico concedida con una antelación superior a tres meses desde la entrada en vigor de este real decreto, y para las cuales no se hubiera solicitado la correspondiente autorización para la puesta en servicio, se entenderá que tienen autorizada dicha puesta en servicio de acuerdo con las características técnicas y condiciones del proyecto técnico aprobado, sin perjuicio del ejercicio de las potestades administrativas de comprobación, inspección, y sanción.

2. Los titulares de derechos de uso del dominio público radioeléctrico que dispongan de la aprobación del proyecto técnico para estaciones de redes y servicios mencionados en el apartado 1 del artículo 53 del reglamento que se aprueba mediante este real decreto, sin que hayan solicitado la autorización para la puesta en servicio de dichas estaciones, dispondrán de un plazo de nueve meses a contar desde la entrada en vigor del presente real decreto, y del reglamento que aprueba, para presentar la citada solicitud de autorización para la puesta en servicio. Esta solicitud de autorización para la puesta en servicio se tramitará conforme a lo dispuesto en el presente real decreto y en el reglamento que aprueba.

Transcurrido el citado plazo sin que el titular de derechos de uso del dominio público radioeléctrico presentase la citada solicitud de autorización para la puesta en servicio, quedará sin efecto la aprobación del proyecto técnico y la correspondiente autorización para realizar la instalación de la estación, y se procederá a su archivo.

Disposición transitoria tercera. *Modelos aprobados conforme a la normativa anterior.*

Los modelos referentes al uso del dominio público radioeléctrico que hubieran sido aprobados por la normativa anterior al presente real decreto y al reglamento que aprueba y, en particular, los modelos de solicitud de título habilitante para el uso del dominio público radioeléctrico y de certificación de estaciones, entre otros, continuarán vigentes en lo que no se opongan al presente real decreto y al reglamento que aprueba, hasta que se aprueben nuevos modelos.

Disposición transitoria cuarta. *Condiciones ligadas a las concesiones de uso de dominio público radioeléctrico.*

Las condiciones ligadas a los títulos habilitantes para el uso del dominio público radioeléctrico destinados a la explotación de redes o prestación de servicios de telecomunicaciones que impliquen el uso del dominio público radioeléctrico, y que se hubieran otorgado con anterioridad a la entrada en vigor del presente real decreto, y del reglamento que aprueba, a través de procedimientos de licitación pública, previstas en los pliegos reguladores de las licitaciones o en la oferta del operador, pasan a estar ligadas a las concesiones de uso privativo de dominio público radioeléctrico.

Disposición transitoria quinta. *Negocios jurídicos formalizados con anterioridad a la entrada en vigor del reglamento aprobado por el presente real decreto, afectados por la regulación del mercado secundario del espectro.*

La modificación, prórroga o renovación de aquellos negocios jurídicos que hayan sido formalizados con anterioridad a la entrada en vigor del reglamento aprobado por el presente real decreto y que, conforme a lo dispuesto en el título VII, deban ser objeto de autorización por la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital por constituir negocios jurídicos relativos al mercado secundario del espectro, debe ser previamente autorizada en los términos establecidos en el citado título.

Disposición derogatoria única. *Derogación normativa.*

Quedan derogadas las siguientes disposiciones:

a) El Real Decreto 863/2008, de 23 de mayo, por el que se aprueba el Reglamento de desarrollo de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, en lo relativo al uso del dominio público radioeléctrico.

b) El Real Decreto 1773/1994, de 5 de agosto, por el que se adecuan determinados procedimientos administrativos en materia de telecomunicaciones a la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

c) Los Capítulos II, IV, V y el anexo I del Reglamento que establece condiciones de protección del dominio público radioeléctrico, restricciones a las emisiones radioeléctricas y medidas de protección sanitaria frente a emisiones radioeléctricas, aprobado mediante el Real Decreto 1066/2001, de 28 de septiembre.

d) Igualmente, quedan derogadas cuantas otras disposiciones de igual o inferior rango se opongan a lo dispuesto en este real decreto.

Disposición final primera. *Modificación de la Orden CTE/23/2002, de 11 de enero, por la que se establecen condiciones para la presentación de determinados estudios y certificaciones por operadores de servicios de radiocomunicaciones.*

1. Se modifica el apartado segundo de la Orden CTE/23/2002, de 11 de enero, por la que se establecen condiciones para la presentación de determinados estudios y certificaciones por operadores de servicios de radiocomunicaciones, que queda redactado de la manera siguiente:

> «Segundo. Tipología de las estaciones radioeléctricas.
>
> 2.1 Tipología de las estaciones radioeléctricas.
>
> Al efecto de lo dispuesto en esta orden, las estaciones radioeléctricas se clasificarán, según su potencia y entorno, en los siguientes tipos:
>
> a) ER1: Estaciones radioeléctricas con potencia isotrópica radiada equivalente máxima superior a 10 vatios, en entorno urbano.
>
> b) ER2: Estaciones radioeléctricas con potencia isotrópica radiada equivalente máxima inferior o igual a 10 vatios y superior a 1 vatio, en entorno urbano.
>
> c) ER3: Estaciones radioeléctricas con potencia isotrópica radiada equivalente máxima superior a 10 vatios, en cuyo entorno no urbano permanecen habitualmente personas.
>
> d) ER4: Estaciones radioeléctricas con potencia isotrópica radiada equivalente máxima inferior o igual a 10 vatios y superior a 1 vatio, en cuyo entorno no urbano permanecen habitualmente personas.
>
> e) ER5: Estaciones radioeléctricas con potencia isotrópica radiada equivalente máxima superior a 1 vatio, en cuyo entorno no urbano no permanecen habitualmente personas.
>
> f) ER6: Estaciones radioeléctricas con potencia isotrópica radiada equivalente máxima inferior o igual a 1 vatio.
>
> 2.2 La permanencia habitual de personas en un entorno determinado consiste en la presencia, estable y prolongada en el tiempo, por parte de una misma persona o personas. Por lo tanto, la circulación o tránsito de personas por un lugar determinado no constituye permanencia habitual de personas.
>
> El entorno queda definido como el área en planta comprendida en un radio de 100 metros desde la estación radioeléctrica. Así, una estación situada en entorno urbano será aquella en la que en un radio de 100 metros haya suelo urbano.
>
> Para identificar el suelo urbano se podrá utilizar como referencia el Sistema de Información Urbana (SIU), conforme a la disposición adicional primera del Real Decreto Legislativo 7/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley de Suelo y Rehabilitación Urbana».

2. El apartado segundo de la Orden CTE/23/2002, de 11 de enero, por la que se establecen condiciones para la presentación de determinados estudios y certificaciones por operadores de servicios de radiocomunicaciones, en los términos en que ha sido redactado en el apartado anterior de esta disposición, podrá ser modificado mediante orden del Ministro de Energía, Turismo y Agenda Digital.

3. Se suprime el apartado séptimo sobre estaciones radioeléctricas con potencia isotrópica radiada equivalente igual o inferior a 1 vatio, que había sido añadido por la Orden ITC/749/2010, de 17 de marzo.

4. Se renumeran los apartados octavo y noveno pasando a numerarse como séptimo y octavo, respectivamente.

Disposición final segunda. *Facultades de desarrollo.*

1. Se autoriza al Ministro de Energía, Turismo y Agenda Digital, en el ámbito de sus competencias, a dictar las disposiciones necesarias para el desarrollo y aplicación de este real decreto, en especial, para modificar o actualizar el contenido de los anexos del reglamento. No obstante, la modificación de la relación de bandas de frecuencias a la que hace referencia su disposición adicional primera y su anexo 1 requerirán el informe previo de la Comisión Nacional de los Mercados y la Competencia, y el acuerdo previo de la Comisión Delegada del Gobierno para Asuntos Económicos.

2. Asimismo, se autoriza a la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital para aprobar mediante resolución los modelos de solicitud para la obtención de títulos habilitantes para el uso del dominio público radioeléctrico, de declaraciones responsables, de solicitud de autorización para la instalación de estaciones radioeléctricas, de solicitud de autorización para la puesta en servicio, de certificaciones sustitutivas de los actos de reconocimiento técnico de las instalaciones previo a la autorización para la puesta en servicio, de informes de medidas, así como sus posibles modificaciones y documentación relacionada, que deberán ponerse a disposición de los ciudadanos a través de la sede electrónica del Ministerio de Energía, Turismo y Agenda Digital.

Disposición final tercera. *Título competencial.*

Este real decreto se dicta al amparo de la competencia exclusiva del Estado sobre telecomunicaciones reconocida en el artículo 149.1.21.ª de la Constitución.

Disposición final cuarta. *Entrada en vigor.*

El presente real decreto entrará en vigor a los veinte días de su publicación en el «Boletín Oficial del Estado».

REGLAMENTO SOBRE EL USO DEL DOMINIO PÚBLICO RADIOELÉCTRICO

TÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

El presente reglamento tiene por objeto el desarrollo de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones (Ley General de Telecomunicaciones), en lo relativo al uso del dominio público radioeléctrico.

Artículo 2. *Principios.*

Los principios que inspiran el presente reglamento son los siguientes:

a) Garantizar, mediante una administración adecuada, el uso eficaz, eficiente y flexible del dominio público radioeléctrico como factor de crecimiento económico, de seguridad y de interés público, social y cultural.

b) Fomentar la competencia efectiva en el mercado de las comunicaciones electrónicas, y facilitar la entrada de nuevos actores en el mercado, garantizando un acceso equitativo a los recursos radioeléctricos mediante procedimientos abiertos, transparentes, objetivos, no discriminatorios, y proporcionados, y a través del desarrollo del mercado secundario y del uso compartido del espectro.

c) Promover la inversión eficiente, la certidumbre regulatoria, y el despliegue territorial de infraestructuras y redes, que faciliten la prestación de servicios de calidad.

d) Favorecer el desarrollo de nuevos servicios y redes y de tecnologías innovadoras, y el acceso a los mismos por parte de todos los ciudadanos, en particular mediante el fomento de la neutralidad tecnológica y de servicios en el uso del espectro.

e) Contribuir al uso armonizado del espectro en el ámbito de la Unión Europea, y facilitar la introducción de sistemas de comunicaciones globales.

f) Garantizar la disponibilidad de espectro para servicios públicos que generan importantes externalidades positivas para la sociedad, en particular, de las comunicaciones relacionadas con la defensa y seguridad nacional, la seguridad pública y los servicios de protección civil y emergencias.

Artículo 3. *Concepto de dominio público radioeléctrico.*

A los efectos del presente reglamento, se considera dominio público radioeléctrico el espacio por el que pueden propagarse las ondas radioeléctricas. Se entiende por espectro radioeléctrico las ondas electromagnéticas cuya frecuencia se fija convencionalmente por debajo de 3.000 gigahertzios que se propagan por el espacio sin guía artificial.

La utilización de ondas electromagnéticas en frecuencias superiores a 3.000 gigahertzios y propagadas por el espacio sin guía artificial se somete al mismo régimen que la utilización de las ondas radioeléctricas, siendo de aplicación lo dispuesto en la Ley General de Telecomunicaciones y en el presente reglamento.

El término frecuencia utilizado en el presente reglamento debe entenderse referido tanto a un valor concreto como a la identificación de la porción de espectro necesario para efectuar una determinada comunicación radioeléctrica (ancho de banda en un canal radioeléctrico).

Artículo 4. *Administración del dominio público radioeléctrico.*

1. La administración del dominio público radioeléctrico le corresponde al Estado, al amparo del artículo 149.1.21.ª de la Constitución, y tiene como objetivo el establecimiento de un marco jurídico que asegure unas condiciones armonizadas para su uso y que permita su disponibilidad y uso eficiente, y abarca un conjunto de actuaciones entre las cuales se incluyen las siguientes:

a) Planificación: Elaboración y aprobación de los planes de utilización del dominio público radioeléctrico.

b) Gestión: Establecimiento, de acuerdo con la planificación previa, de las condiciones técnicas de explotación y otorgamiento de los derechos de uso.

c) Control: Comprobación técnica de las emisiones radioeléctricas y su adecuación a los derechos de uso otorgados y a los parámetros técnicos de utilización, localización y eliminación de interferencias perjudiciales, infracciones, irregularidades y perturbaciones de los sistemas de radiocomunicaciones, la verificación del uso efectivo y eficiente del dominio público radioeléctrico por parte de los titulares de derechos de uso, análisis de los niveles de exposición radioeléctrica, inspección técnica de instalaciones, equipos y aparatos radioeléctricos, así como el control de la puesta en el mercado de éstos últimos.

Asimismo, dentro de la actuación de control se encuentra la protección activa del dominio público radioeléctrico, consistente, entre otras actuaciones, en la realización de emisiones sin contenidos sustantivos en aquellas frecuencias y canales radioeléctricos cuyos derechos de uso, en el ámbito territorial correspondiente, no hayan sido otorgados, con independencia de que dichas frecuencias o canales radioeléctricos sean objeto en la práctica de ocupación o uso efectivo.

d) Aplicación del régimen sancionador.

2. La utilización de frecuencias radioeléctricas mediante redes de satélites se incluye dentro de la administración del dominio público radioeléctrico

TÍTULO II

Planificación del dominio público radioeléctrico

Artículo 5. *Planes de utilización del dominio público radioeléctrico.*

1. La utilización del dominio público radioeléctrico se efectuará de acuerdo con una planificación previa, delimitando, en su caso, las bandas y canales atribuidos a cada uno de los servicios.

2. Son planes de utilización del dominio público radioeléctrico el Cuadro Nacional de Atribución de Frecuencias (CNAF), los planes técnicos nacionales de radiodifusión sonora y de televisión cuya aprobación corresponderá al Gobierno, y los aprobados por otras normas con rango mínimo de orden ministerial.

3. Corresponde a la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital la elaboración de las propuestas de planes de utilización del dominio público radioeléctrico y su tramitación, elevándolos al órgano competente para su aprobación.

Artículo 6. *Cuadro Nacional de Atribución de Frecuencias (CNAF).*

1. A fin de lograr la utilización coordinada y eficaz del dominio público radioeléctrico, el Ministro de Energía, Turismo y Agenda Digital aprobará el Cuadro Nacional de Atribución de Frecuencias para los diferentes tipos de servicios de radiocomunicación, de acuerdo con las disposiciones de la Unión Europea, de la Conferencia Europea de Administraciones de Correos y Telecomunicaciones (CEPT), y del Reglamento de Radiocomunicaciones de la Unión Internacional de Telecomunicaciones (UIT), definiendo la atribución de bandas, subbandas, frecuencias, y canales, así como las demás características técnicas que pudieran ser necesarias. Asimismo, el Cuadro Nacional de Atribución de Frecuencias podrá establecer los tipos y condiciones de uso aplicables a cada banda de frecuencias.

El Cuadro Nacional de Atribución de Frecuencias podrá establecer, entre otras, las siguientes previsiones:

a) Reservar parte del dominio público radioeléctrico para servicios determinados.

b) Establecer preferencias de uso por razón del fin social del servicio a prestar.

c) Delimitar las bandas, canales o frecuencias que se reservan a las Administraciones Públicas, o entes públicos de ellas dependientes, para la gestión directa de sus servicios.

d) Establecer las bandas, subbandas o frecuencias que se destinarán al uso privativo del dominio público radioeléctrico.

e) Establecer las bandas, subbandas o frecuencias que tengan la consideración de uso común del dominio público radioeléctrico.

f) Fomentar la neutralidad tecnológica y de los servicios en la explotación del dominio público radioeléctrico.

g) Fijar para determinadas bandas o subbandas de frecuencias, o conjuntos de bandas, límites a la cantidad de espectro que podrá ser reservado en favor de un mismo titular, cuando sea necesario para promover la competencia en la prestación de los servicios, garantizar el acceso equitativo al uso del espectro, o evitar comportamientos especulativos o acaparamiento de derechos de uso del dominio público radioeléctrico.

2. En el proceso de elaboración del Cuadro Nacional de Atribución de Frecuencias será de aplicación el procedimiento de elaboración de disposiciones administrativas de carácter general. La Secretaría de Estado para la Sociedad de la Información y la Agenda Digital someterá a consulta pública los proyectos correspondientes. En el caso de que se modifiquen los límites a la cantidad de espectro que podrá ser reservado en favor de un mismo titular a que se refiere el párrafo g) del apartado anterior, se recabará el informe previo de la Comisión Delegada del Gobierno para Asuntos Económicos.

3. En las bandas de radiofrecuencias declaradas disponibles para la prestación de los servicios de comunicaciones electrónicas en el Cuadro Nacional de Atribución de

Frecuencias, se podrá emplear cualquier tipo de tecnología de conformidad con el Derecho de la Unión Europea.

No obstante, podrán preverse restricciones proporcionadas y no discriminatorias a los tipos de tecnología de acceso inalámbrico o red radioeléctrica utilizados para los servicios de comunicaciones electrónicas en estas bandas cuando sea necesario para los siguientes casos:

a) Evitar interferencias perjudiciales.
b) Proteger la salud pública frente a los campos electromagnéticos.
c) Asegurar la calidad técnica del servicio.
d) Garantizar un uso compartido máximo de las radiofrecuencias.
e) Garantizar un uso eficiente del espectro.
f) Garantizar el logro de un objetivo de interés general.

4. En las bandas de radiofrecuencias declaradas disponibles para la prestación de los servicios de comunicaciones electrónicas en el Cuadro Nacional de Atribución de Frecuencias, se podrá prestar cualquier tipo de servicios de comunicaciones electrónicas, de conformidad con el Derecho de la Unión Europea.

No obstante, podrán preverse restricciones, proporcionadas y no discriminatorias a los tipos de servicios de comunicaciones electrónicas que se presten en estas bandas, incluido, cuando proceda, el cumplimiento de algún requisito del Reglamento de Radiocomunicaciones de la UIT.

Las medidas que exijan que un servicio de comunicaciones electrónicas se preste en una banda específica disponible para los servicios de comunicaciones electrónicas deberán estar justificadas.

Únicamente se impondrá la atribución específica de una banda de frecuencias para la prestación de un determinado servicio de comunicaciones electrónicas cuando esté justificado por la necesidad de proteger servicios relacionados con la seguridad de la vida o, excepcionalmente, cuando sea necesario para alcanzar objetivos de interés general definidos con arreglo al Derecho de la Unión Europea, tales como:

a) La seguridad de la vida.
b) La promoción de la cohesión social, regional o territorial.
c) La evitación del uso ineficiente de las radiofrecuencias.
d) La promoción de la diversidad cultural y lingüística y del pluralismo de los medios de comunicación, mediante, por ejemplo, la prestación de servicios de radiodifusión sonora y de televisión.

5. Las restricciones a la utilización de bandas de frecuencias que, en su caso, se establezcan de conformidad con los apartados anteriores sólo podrán adoptarse previo trámite de audiencia a las partes interesadas en los términos establecidos en el artículo 82 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Cuando varíen las circunstancias que aconsejaron su establecimiento, la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital revisará la pertinencia de mantener las restricciones a la utilización de bandas de frecuencias que, en su caso, se hubieran establecido de conformidad con los apartados anteriores, hará públicos los resultados de estas revisiones y elevará las propuestas correspondientes al órgano competente para su aprobación.

Artículo 7. *Planes técnicos nacionales de radiodifusión sonora y de televisión.*

1. Corresponde a la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital la elaboración de los proyectos de los planes técnicos nacionales de radiodifusión sonora y de televisión, conforme lo establecido en este artículo, elevándolos al Gobierno para su aprobación.

Los proyectos de los planes técnicos nacionales de radiodifusión sonora y de televisión serán elaborados con el objetivo de alcanzar una utilización racional, óptima y eficaz del dominio público radioeléctrico.

2. Los planes técnicos nacionales de radiodifusión sonora y de televisión establecerán, al menos, las frecuencias de emisión, los bloques de frecuencias o, en su caso, los canales radioeléctricos y las condiciones para proporcionar servicios de calidad técnica satisfactoria en las zonas de servicio que hayan sido expresamente definidas, así como cualquier otro parámetro técnico de referencia u otras disposiciones administrativas que resulten necesarias.

En el proceso de elaboración de los planes técnicos nacionales de radiodifusión sonora y de televisión se asegurará la participación de las Comunidades Autónomas, en los términos previstos en la Ley 7/2010, de 31 de marzo, General de la Comunicación Audiovisual, cuando se refieran a servicios cuyos títulos habilitantes para prestación de servicios audiovisuales corresponda otorgar a las Comunidades Autónomas. A estos efectos los planes técnicos serán informados por el Consejo Asesor de las Telecomunicaciones y de la Sociedad de la Información.

Artículo 8. *Registro Nacional de Frecuencias.*

1. La Secretaría de Estado para la Sociedad de la Información y la Agenda Digital gestionará un registro de los derechos de uso de frecuencias que hubieran sido autorizados conforme a lo previsto en este reglamento. En dicho registro se inscribirán, además de los datos del titular del derecho de uso del dominio público radioeléctrico otorgado, las características técnicas de explotación de dicho derecho de uso.

2. De acuerdo con lo establecido en el artículo 10.2 de la Ley General de Telecomunicaciones y en conformidad con la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, para garantizar la protección del secreto comercial o industrial de los titulares de derechos de uso del dominio público radioeléctrico y la seguridad pública, no se facilitará información de los datos inscritos en el registro, diferentes de los incluidos en el Registro Público de Concesiones al que se refiere el artículo siguiente, sin perjuicio de la colaboración que deba prestarse al Centro Nacional de Inteligencia en virtud de lo establecido en el artículo 5.5 de la Ley 11/2002, de 6 de mayo, reguladora del CNI. El acceso directo a todo o a parte del registro quedará restringido a las personas que designe la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital.

Asimismo, para garantizar los intereses relacionados con la defensa nacional, el acceso directo al registro sobre los usos de las frecuencias vinculados a la misma quedará restringido a las personas que designen conjuntamente el Ministerio de Defensa y la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital.

Artículo 9. *Registro Público de Concesiones.*

La Secretaría de Estado para la Sociedad de la Información y la Agenda Digital gestionará un registro público, accesible a través de la sede electrónica del Ministerio de Energía, Turismo y Agenda Digital, en el que constarán los datos públicos del Registro Nacional de Frecuencias relativos a los titulares de concesiones administrativas para el uso privativo del dominio público radioeléctrico. En este registro público de concesiones se incluirán los siguientes datos:

a) Referencia de la concesión.
b) Nombre o razón social, domicilio y número de identificación fiscal del titular.
c) Fecha de otorgamiento y caducidad de la concesión.
d) Ámbito geográfico y tipo de servicio autorizado.
e) Frecuencia o banda de frecuencias reservadas.
f) Indicación sobre si los derechos de uso del dominio público radioeléctrico de la concesión son susceptibles de cesión a terceros o mutualización.
g) Indicación, en su caso, de si los derechos de uso del dominio público radioeléctrico han sido obtenidos mediante un procedimiento de transferencia de título, así como el nombre o razón social y el número o código de identificación fiscal del titular que transfiere el título.
h) Indicación, en su caso, de si los derechos de uso del dominio público radioeléctrico a que habilita la concesión son objeto de cesión, así como el nombre o razón social y el número o código de identificación fiscal del titular al que se ceden los derechos de uso.

i) Indicación, en su caso, de si los derechos de uso del dominio público radioeléctrico a que habilita la concesión son objeto de mutualización, así como el nombre o razón social y el número o código de identificación fiscal del otro u otros mutualistas.

TÍTULO III

Uso del dominio público radioeléctrico

CAPÍTULO I

Disposiciones comunes a los diferentes usos del dominio público radioeléctrico

Artículo 10. *Tipos de uso del dominio público radioeléctrico.*

1. El uso del dominio público radioeléctrico puede ser común, especial o privativo, quedando en todos los casos sometido a las disposiciones contenidas en este reglamento.
2. El uso común del dominio público radioeléctrico no precisará de ningún título habilitante para el uso de dicho dominio, y se llevará a cabo en las bandas de frecuencias y con las características técnicas que se establezcan en el Cuadro Nacional de Atribución de Frecuencias.
3. El uso especial del dominio público radioeléctrico es el que se lleva a cabo de las bandas de frecuencias habilitadas para su explotación de forma compartida, sin limitación de número de operadores o usuarios, y con las condiciones técnicas y para los servicios que se establezcan en cada caso.
4. El uso privativo del dominio público radioeléctrico es el que se realiza mediante la explotación, en exclusiva o por un número limitado de usuarios, de determinadas frecuencias en un mismo ámbito físico de aplicación.

Artículo 11. *Títulos habilitantes para el uso del dominio público radioeléctrico.*

1. El uso del dominio público radioeléctrico requerirá la previa obtención de título habilitante, salvo en los casos de uso común.
2. Los títulos habilitantes mediante los que se otorguen derechos de uso del dominio público radioeléctrico revestirán la forma de autorización general, autorización individual, afectación o concesión administrativa.
3. El otorgamiento de derechos de uso del dominio público radioeléctrico revestirá la forma de autorización general en los supuestos de uso especial de las bandas de frecuencia habilitadas, a tal efecto, a través de redes públicas de comunicaciones electrónicas instaladas o explotadas por operadores de comunicaciones electrónicas.
4. El otorgamiento de derechos de uso del dominio público radioeléctrico revestirá la forma de autorización individual en los siguientes supuestos:

a) Si se trata de una reserva de derecho de uso especial por radioaficionados, u otros sin contenido económico en cuya regulación específica así se establezca.
b) Si se otorga el derecho de uso privativo para autoprestación por el solicitante, salvo en el caso de administraciones públicas, que requerirán de afectación demanial.

5. En el resto de supuestos no contemplados en los apartados anteriores, el derecho al uso privativo del dominio público radioeléctrico requerirá una concesión administrativa.
6. El plazo para el otorgamiento de los títulos habilitantes para el uso del dominio público radioeléctrico será de seis semanas desde la entrada de la solicitud en cualquiera de los registros del órgano administrativo competente, sin perjuicio de lo establecido para los derechos de uso con limitación de número. Dicho plazo no será de aplicación cuando sea necesaria la coordinación internacional de frecuencias o afecte a reservas de posiciones orbitales.

Transcurrido el plazo sin haberse notificado resolución expresa, deberán entenderse desestimadas las solicitudes, sin perjuicio de la obligación de la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital de resolver expresamente, de acuerdo con lo

dispuesto en el artículo 24 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Artículo 12. *Uso eficaz y uso eficiente del dominio público radioeléctrico.*

1. A los efectos del presente reglamento, se entenderá que los derechos de uso del dominio público radioeléctrico otorgados se utilizan eficazmente cuando su uso sea efectivo y continuado en las zonas geográficas para las que fue reservado, sin perjuicio de las reservas destinadas a situaciones de emergencia o relacionadas con la defensa nacional, la seguridad u otros servicios esenciales.

2. Se entenderá por uso eficiente del dominio público radioeléctrico aquel que proporciona un menor consumo de recursos espectrales, garantizando los mismos objetivos de cobertura, capacidad de transmisión y calidad del servicio.

3. El uso eficaz y eficiente del dominio público radioeléctrico son condiciones exigibles a los titulares de derechos de uso del dominio público durante la vigencia de los correspondientes títulos habilitantes para el uso del dominio público radioeléctrico.

Artículo 13. *Uso compartido del dominio público radioeléctrico.*

1. El uso compartido del dominio público radioeléctrico permite el uso de una banda o rango de frecuencias por parte de varios usuarios, a los que se otorgan derechos de uso de dichas frecuencias en un mismo ámbito geográfico.

2. Los titulares de derechos de uso de frecuencias, bandas o subbandas del dominio público radioeléctrico que, en el Cuadro Nacional de Atribución de Frecuencias, se establezcan como de uso compartido con otros titulares, habrán de aceptar las limitaciones y restricciones inherentes a dicho régimen de asignación de frecuencias, incorporando a sus redes los dispositivos técnicos pertinentes.

3. Asimismo, y en aras de alcanzar un uso más eficiente del dominio público radioeléctrico, podrá imponerse el uso compartido del espectro radioeléctrico por terceros a los titulares de derechos de uso de espectro en las bandas de frecuencia que así se determine, en los siguientes casos:

a) En las zonas geográficas en las que exista una infrautilización de los derechos de uso otorgados.

b) Cuando la utilización de tecnologías apropiadas permitan el otorgamiento de derechos de uso compartidos, de manera compatible con los derechos de uso anteriormente otorgados. El acceso compartido bajo esta modalidad se efectuará de acuerdo con la normativa comunitaria sobre armonización de uso del espectro radioeléctrico, y no deberá suponer un menoscabo de los derechos de uso atribuidos inicialmente.

Artículo 14. *Conformidad de los equipos y de las instalaciones.*

Todos los equipos y aparatos que utilicen el espectro radioeléctrico deberán cumplir con lo previsto en la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, y su normativa de desarrollo y, en particular, haber evaluado su conformidad y cumplir el resto de requisitos que le son aplicables, en los términos recogidos en el Real Decreto 188/2016, de 6 de mayo, por el que se aprueba el Reglamento por el que se establecen los requisitos para la comercialización, puesta en servicio y uso de equipos radioeléctricos, y se regula el procedimiento para la evaluación de la conformidad, la vigilancia del mercado y el régimen sancionador de los equipos de telecomunicación, y en el Real Decreto 186/2016, de 6 de mayo, por el que se regula la compatibilidad electromagnética de los equipos eléctricos y electrónicos. Igualmente, deberán respetar lo especificado en el Cuadro Nacional de Atribución de Frecuencias, así como en las interfaces radioeléctricas en vigor.

CAPÍTULO II

Estaciones radioeléctricas y su instalación y operación

Artículo 15. *Estaciones que utilizan el dominio público radioeléctrico.*

1. A efectos de la utilización del dominio público radioeléctrico, una estación radioeléctrica está formada por uno o más transmisores o receptores, o una combinación de ambos, incluyendo las instalaciones accesorias o necesarias para asegurar, en un lugar determinado, un servicio de radiocomunicación o el servicio de radioastronomía.

2. Las estaciones radioeléctricas, según su movilidad, se pueden clasificar en las siguientes categorías:

a) Estación fija: Estación destinada a un uso permanente en un determinado emplazamiento.

b) Estación móvil: Estación a bordo de un vehículo destinada a ser utilizada en movimiento o, mientras esté detenida, en puntos no determinados.

c) Estación portátil: Estación transportable por una persona destinada a ser utilizada en movimiento o, mientras esté detenida, en puntos no determinados.

Artículo 16. *Instalación de estaciones radioeléctricas.*

1. Para la instalación y posterior utilización de estaciones radioeléctricas, el titular deberá haber obtenido el correspondiente título habilitante para el uso del dominio público radioeléctrico, salvo en los casos en que la instalación haga un uso común del dominio público radioeléctrico.

2. Antes de realizar una instalación que vaya a hacer uso del dominio público radioeléctrico, el titular deberá obtener de la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital la aprobación del proyecto técnico de la estación, o de la red de estaciones a instalar, y la consiguiente autorización para realizar la instalación, de acuerdo con lo previsto en el presente reglamento.

3. Una vez realizada la instalación, con carácter previo a la utilización del dominio público radioeléctrico, el titular deberá obtener la autorización para la puesta en servicio de la estación, o de la red de estaciones, después de efectuada la inspección o el reconocimiento favorable de las instalaciones en los casos y condiciones establecidos en el presente reglamento.

Artículo 17. *Instalación y operación de estaciones radioeléctricas por parte de terceros.*

1. Los titulares de derechos de uso del dominio público radioeléctrico podrán otorgar poderes bastantes a un tercero para que sea este último quien realice la instalación, operación o mantenimiento de las estaciones radioeléctricas correspondientes.

Cuando un operador reciba el encargo de efectuar emisiones radioeléctricas por parte de personas o entidades que ostenten el correspondiente título habilitante para el uso del dominio público radioeléctrico, deberá comunicárselo previamente a la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital y efectuar dichas emisiones de acuerdo con las condiciones y características técnicas autorizadas por la Administración.

El titular de los derechos de uso del dominio público radioeléctrico será el responsable de que, la instalación y la utilización de la estación radioeléctrica, se realiza en conformidad con las condiciones autorizadas.

2. El tercero encargado de la operación o mantenimiento de las estaciones radioeléctricas, podrá presentar, en nombre del titular o titulares, las solicitudes de autorización para la instalación, los proyectos técnicos o las declaraciones responsables correspondientes, las solicitudes de autorización para la puesta en servicio de las estaciones, y las certificaciones anuales, en el caso de que sean necesarias, de acuerdo con este reglamento.

3. De acuerdo con lo establecido en el artículo 62.10 de la Ley General de Telecomunicaciones, los operadores que vayan a efectuar emisiones radioeléctricas mediante el uso del dominio público radioeléctrico por encargo de otras personas o entidades, deberán verificar, previamente al inicio de dichas emisiones, que las entidades a

cuya disposición ponen su red ostentan el correspondiente título habilitante para ese uso del dominio público radioeléctrico. Los operadores no podrán poner a disposición de las entidades referidas su red y, en consecuencia, no podrán dar el acceso a su red a dichas entidades ni podrán efectuar las mencionadas emisiones en caso de ausencia del citado título habilitante para la prestación del servicio encargado.

Artículo 18. *Otros requisitos previos para la instalación y para la puesta en servicio de estaciones radioeléctricas.*

La aprobación del proyecto técnico y la correspondiente autorización para realizar la instalación, así como la posterior inspección o el reconocimiento favorable de las instalaciones, y la consiguiente autorización para la puesta en servicio de las estaciones otorgada por la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital, corresponde exclusivamente al ámbito de las condiciones de uso del dominio público radioeléctrico, y no supone el cumplimiento de otros requisitos, o el otorgamiento de permisos, autorizaciones o presentación de declaraciones responsables que, de acuerdo con la legislación vigente, puedan ser exigibles, y que el titular de los derechos de uso del dominio público radioeléctrico deberá solicitar y obtener de los órganos competentes. En particular, será necesaria la autorización de seguridad aérea, cuando resulte exigible de acuerdo con lo establecido en la normativa específica sobre esta materia.

CAPÍTULO III

Uso común del dominio público radioeléctrico

Artículo 19. *Concepto de uso común del dominio público radioeléctrico.*

1. El uso común del dominio público radioeléctrico es el que se realiza sin precisar ningún título habilitante, sin limitación de número de operadores o usuarios, y con las condiciones técnicas que se determinen en el Cuadro Nacional de Atribución de Frecuencias.

2. Se destinarán al uso común del dominio público radioeléctrico:

a) Aquellas bandas, subbandas o frecuencias que se señalen para dicho uso en el Cuadro Nacional de Atribución de Frecuencias.

b) La utilización de aquellas bandas, subbandas o frecuencias que se señalen como tales en el Cuadro Nacional de Atribución de Frecuencias para aplicaciones industriales, científicas y médicas (ICM).

Artículo 20. *Régimen jurídico del uso común del dominio público radioeléctrico.*

1. El uso común del dominio público radioeléctrico no precisará de título habilitante y se ejercerá con sujeción a lo dispuesto en este reglamento.

2. El uso común del dominio público radioeléctrico deberá realizarse en los términos y condiciones técnicas establecidas en el Cuadro Nacional de Atribución de Frecuencias.

3. Los servicios que efectúen un uso común del dominio público radioeléctrico no deberán producir interferencias perjudiciales a otros servicios de radiocomunicaciones autorizados, ni podrán solicitar protección frente a ellos.

4. La utilización de estaciones radioeléctricas correspondientes a este tipo de uso se considerará autorizada con carácter general, siempre que se cumpla con los términos y condiciones técnicas establecidas en el Cuadro Nacional de Atribución de Frecuencias y las señaladas con carácter general en este reglamento.

Artículo 21. *Limitación de los derechos de uso común.*

Por razones de eficiencia en el uso del dominio público radioeléctrico o por razones técnicas de atribución de bandas, el Cuadro Nacional de Atribución de Frecuencias podrá modificar el carácter de uso común de determinadas bandas, subbandas o frecuencias, y establecer su atribución para otros tipos de uso.

En dicho supuesto, en la orden de modificación del Cuadro Nacional de Atribución de Frecuencias, se señalará un período transitorio de adaptación, no originando, en ningún caso, derecho de indemnización a los actuales usuarios y siendo por cuenta de éstos los costes de adaptación a la normativa que esto pudiera suponer.

CAPÍTULO IV

Uso especial del dominio público radioeléctrico

Artículo 22. *Concepto de uso especial del dominio público radioeléctrico.*

1. El uso especial del dominio público radioeléctrico es el que se realiza mediante la explotación de forma compartida, sin limitación de número de operadores o usuarios, con las condiciones y para los servicios que se establezcan en cada caso, y con las condiciones técnicas que se determinen en el Cuadro Nacional de Atribución de Frecuencias o en su regulación específica.
2. Se destinarán al uso especial del dominio público radioeléctrico aquellas bandas, subbandas o frecuencias que se señalen para dicho uso en el Cuadro Nacional de Atribución de Frecuencias.

Artículo 23. *Título habilitante para el uso especial del dominio público radioeléctrico.*

De acuerdo con lo establecido en el artículo 62 de la Ley General de Telecomunicaciones, los títulos habilitantes mediante los que se otorguen derechos de uso especial del dominio público radioeléctrico revestirán la forma de autorización general o autorización individual.

Artículo 24. *Autorización general para el uso especial del dominio público radioeléctrico.*

1. El otorgamiento de derechos de uso especial del dominio público radioeléctrico revestirá la forma de autorización general en los supuestos de uso especial de las bandas de frecuencias, habilitadas a tal efecto, mediante redes públicas de comunicaciones electrónicas instaladas o explotadas por prestadores de servicios de comunicaciones electrónicas.
2. Dicha autorización general se entenderá concedida sin más trámite que la notificación a la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital, mediante el procedimiento y con los requisitos que se establezcan mediante orden ministerial, sin perjuicio de la obligación de abono de las tasas correspondientes. Cuando la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital constate que la notificación no reúne los requisitos anteriores, dictará resolución motivada en un plazo máximo de quince días, no teniéndose por realizada aquella.
3. La utilización de estaciones radioeléctricas correspondientes a este tipo de uso se considerará autorizada con carácter general, siempre que cumplan con los términos y condiciones técnicas establecidas para las mismas, y las señaladas con carácter general en este reglamento.

Artículo 25. *Autorización individual para el uso especial del dominio público radioeléctrico.*

1. El otorgamiento de derechos de uso especial del dominio público radioeléctrico revestirá la forma de autorización individual si se trata de una reserva de derecho de uso especial por radioaficionados u otros sin contenido económico, en cuya regulación específica o en el Cuadro Nacional de Atribución de Frecuencias así se establezca.
2. Mediante orden ministerial se establecerán las condiciones de explotación y de otorgamiento de la autorización individual de uso especial del dominio público radioeléctrico.
3. Las autorizaciones individuales se otorgarán por orden de presentación de solicitudes, sin más limitaciones que las que se deriven de la política y buena gestión del dominio público radioeléctrico, sin perjuicio de derechos de terceros usuarios del dominio público.

Artículo 26. *Proyecto técnico y autorización para realizar la instalación de estaciones de uso especial del dominio público radioeléctrico en el caso de las autorizaciones individuales.*

1. Las estaciones radioeléctricas destinadas a su utilización por los titulares de autorizaciones individuales de uso especial del dominio público radioeléctrico podrán ser estaciones fijas, móviles y portátiles.

2. Para realizar la instalación de las estaciones fijas los titulares deberán presentar ante la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital un proyecto técnico de la estación, y obtener la correspondiente aprobación del proyecto técnico, con las modificaciones que en su caso resultaran necesarias. La aprobación del proyecto técnico en la que se determinarán las características técnicas de la estación, incluirá la autorización para realizar la instalación de acuerdo con las características aprobadas.

Transcurrido el plazo de seis meses sin que se haya notificado la aprobación del proyecto técnico y autorizada la realización de la instalación, deberá entenderse desestimada dicha solicitud, sin perjuicio de la obligación de la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital de resolver expresamente, de acuerdo con lo dispuesto en el artículo 24 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

3. Mediante orden del Ministro de Energía, Turismo y Agenda Digital se determinará el procedimiento para la tramitación de dichas solicitudes, así como el contenido a que habrá de ajustarse el proyecto técnico correspondiente.

4. La utilización de estaciones móviles o portátiles a que se refiere este artículo no precisa de autorización, siempre que se cumplan las características técnicas especificadas mediante orden ministerial y en el resto de la normativa vigente.

Artículo 27. *Limitación de los derechos de uso especial.*

Por razones de eficiencia en el uso del dominio público radioeléctrico o por razones técnicas de atribución de bandas, el Cuadro Nacional de Atribución de Frecuencias podrá modificar el carácter de uso especial de determinadas bandas, subbandas o frecuencias, y establecer su atribución para otros usos. La orden de aprobación o de modificación del Cuadro Nacional de Atribución de Frecuencias justificará debidamente dichas razones.

Adicionalmente, en dicha orden, se señalará un período transitorio de adaptación, no originando, en ningún caso, derecho de indemnización a los actuales usuarios y siendo por cuenta de éstos los costes de adaptación a la normativa que esto pudiera suponer.

CAPÍTULO V

Uso privativo del dominio público radioeléctrico

Sección 1.ª Normas generales

Artículo 28. *Concepto del uso privativo del dominio público radioeléctrico.*

1. El uso privativo del dominio público radioeléctrico es el que se realiza mediante la explotación, en exclusiva o por un número limitado de usuarios, de determinadas frecuencias en un mismo ámbito físico de aplicación.

2. Las asignaciones de frecuencias para el uso privativo del dominio público radioeléctrico se efectuarán, en cualquier caso, para la prestación de los servicios o el ejercicio de las actividades especificadas en el correspondiente título habilitante para el uso del dominio público radioeléctrico.

Artículo 29. *Títulos habilitantes para el uso privativo del dominio público radioeléctrico.*

1. De acuerdo con el artículo 62 de la Ley General de Telecomunicaciones, el otorgamiento del derecho de uso privativo del dominio público radioeléctrico revestirá alguna de las formas siguientes:

a) Autorización individual.
b) Afectación demanial.

c) Concesión administrativa.

2. La autorización individual se otorgará en los casos de uso privativo del dominio público radioeléctrico destinados a la autoprestación de servicios, a las emisiones con fines experimentales y a las emisiones para eventos de corta duración.

La afectación demanial se otorgará en el caso de uso privativo del dominio público radioeléctrico destinado a la autoprestación de servicios por parte de las Administraciones Públicas.

No se otorgarán derechos de uso privativo del dominio público radioeléctrico para su uso en autoprestación en los supuestos en los que la demanda supere a la oferta y se aplique el procedimiento de licitación previsto en el artículo 63 de la Ley General de Telecomunicaciones.

En los restantes supuestos, el derecho al uso privativo del dominio público radioeléctrico requerirá una concesión administrativa. Para el otorgamiento de dicha concesión administrativa, los solicitantes deberán reunir los siguientes requisitos previos:

a) Ostentar la condición de operador de comunicaciones electrónicas.

b) No incurrir en ninguna de las prohibiciones de contratar reguladas en el texto refundido de la Ley de Contratos del Sector Público, aprobado mediante el Real Decreto Legislativo 3/2011, de 14 de noviembre.

c) Haber realizado el pago de las tasas correspondientes a la tramitación de la concesión administrativa y otros requisitos económicos que sean exigibles.

3. Las concesiones de uso privativo del dominio público radioeléctrico reservado para la prestación de servicios de radiodifusión sonora y de televisión por ondas terrestres se otorgarán por la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital anejas al título habilitante para la prestación del servicio de comunicación audiovisual. La duración de estas concesiones será la del título habilitante audiovisual. En estos supuestos, la concesión se otorgará en favor del prestador del servicio de comunicación audiovisual correspondiente, sin que sea necesario que éste ostente la condición de prestador de servicios de comunicaciones electrónicas.

Sección 2.ª Procedimientos de obtención de los títulos habilitantes para uso privativo del dominio público radioeléctrico

Subsección 1.ª Uso privativo del dominio público radioeléctrico sin limitación del número. Procedimiento general

Artículo 30. *Procedimiento de obtención de título habilitante para el uso privativo del dominio público radioeléctrico sin limitación de número, otorgado mediante el procedimiento general.*

1. Los interesados en obtener cualquier título habilitante para el uso privativo del dominio público radioeléctrico sin limitación de número, otorgado mediante el procedimiento general, deberán presentar sus solicitudes conforme a los modelos que, en su caso, se establezcan y la documentación adicional correspondiente ante la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital.

2. Si la documentación aportada no reuniera los requisitos exigidos, se requerirá al interesado para que, en el plazo de diez días hábiles, desde el siguiente al de recepción del requerimiento, subsane la falta o acompañe los documentos preceptivos, con advertencia de que, si no lo hiciese, se le tendrá por desistido de su solicitud, previa resolución de la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital, de acuerdo con lo establecido en el artículo 68 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

3. La Secretaría de Estado para la Sociedad de la Información y la Agenda Digital, antes de dictar la resolución sobre el otorgamiento o denegación del título habilitante necesario para el uso privativo del dominio público radioeléctrico podrá requerir al solicitante cuanta información o aclaraciones considere convenientes sobre su solicitud o sobre los documentos presentados.

Artículo 31. *Documentación administrativa.*

La documentación administrativa a incluir en las solicitudes de títulos habilitantes para uso privativo del dominio público radioeléctrico sin limitación de número estará constituida por los documentos que a continuación se relacionan, entendiéndose presentada aquella documentación que haya sido necesaria acreditar para la obtención y uso del certificado electrónico reconocido:

1. Documentos que acrediten la capacidad del solicitante.

a) Persona física española: Documento Nacional de Identidad (DNI) o, en su defecto, consentimiento para que los datos de identidad personal del interesado puedan ser consultados mediante el Sistema de Verificación de Datos de Identidad Personal, a los efectos de iniciación del procedimiento, de conformidad con lo establecido en la Orden PRE/3949/2006, de 26 de diciembre por la que se establece la configuración, características, requisitos y procedimientos de acceso al Sistema de verificación de datos de identidad.

b) Persona física extranjera: Documento equivalente al DNI en caso de extranjeros, o Número de Identificación Fiscal otorgado por la Agencia Estatal de Administración Tributaria.

c) Persona jurídica: Número de Identificación Fiscal otorgado por la Agencia Estatal de Administración Tributaria.

2. Documentos que acrediten la representación.

a) Los que comparezcan o firmen solicitudes en nombre de otros deberán presentar documento que acredite la representación o, en su caso, poder bastante al efecto debidamente inscrito en el Registro Mercantil, y fotocopia compulsada o legitimada notarialmente de su DNI, o, en su defecto, consentimiento para que los datos de identidad personal del interesado puedan ser consultados mediante el Sistema de Verificación de Datos de Identidad Personal, a los efectos de iniciación del procedimiento, de conformidad con lo establecido en la Orden PRE/3949/2006, de 26 de diciembre, por la que se establece la configuración, características, requisitos y procedimientos de acceso al Sistema de verificación de datos de identidad, o, en el supuesto de ciudadanos extranjeros, del documento equivalente al DNI.

b) Si el solicitante fuese una persona física o jurídica extranjera, deberá designar un representante y aportará el documento que acredite su domiciliación en España, salvo en el caso de los eventos de corta duración a los que se refiere el artículo 48. En ese caso, se entenderá que el domicilio del representante coincide con el domicilio a efectos de notificaciones de la persona representada.

3. Justificante, en su caso, de abono de la tasa de telecomunicaciones por tramitación de concesiones demaniales para el uso privativo del dominio público radioeléctrico establecida en el anexo I.4 de la Ley General de Telecomunicaciones.

4. En el caso de concesión administrativa:

a) Certificación de estar inscrito en el Registro de Operadores previsto en el artículo 7 de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

b) Declaración responsable de no estar incurso el solicitante en ninguna de las prohibiciones de contratar reguladas en el texto refundido de la Ley de Contratos del Sector Público, aprobado mediante el Real Decreto Legislativo 3/2011, de 14 de noviembre.

5. En el caso de solicitudes de título habilitante para el uso privativo de dominio público radioeléctrico para la explotación de redes de comunicaciones electrónicas que utilicen satélites, incluidas las destinadas a la prestación de servicios de radiodifusión sonora y de televisión a través de redes de satélites, deberán acompañar además a su solicitud documento que acredite fehacientemente que el solicitante dispone o está en condiciones de obtener la capacidad de segmento espacial correspondiente a la red radioeléctrica que pretende instalar, proporcionada por el titular de la infraestructura satelital.

6. Asimismo, cuando se solicite el otorgamiento de título habilitante para el uso del dominio público radioeléctrico para el acceso a estaciones terrenas de enlace con una estación espacial, cuya titularidad corresponda a una Administración extranjera, o la prestación de servicios basados en la misma, requerirá igualmente, sin perjuicio de los acuerdos internacionales celebrados por el Estado español, que el solicitante acredite:

a) Que la estación espacial se encuentre inscrita en el Registro Internacional de Frecuencias de la UIT.

b) La existencia de un acuerdo de reciprocidad que reconozca a las personas físicas o jurídicas españolas el derecho a prestar servicios similares en el país del que sea nacional la persona física o jurídica solicitante del título habilitante para el uso del dominio público radioeléctrico, sin perjuicio de lo previsto por los Acuerdos Internacionales suscritos por España o la Unión Europea.

7. Declaración de las personas extranjeras de someterse a la jurisdicción de los Juzgados y Tribunales españoles de cualquier orden para todas las incidencias que, de modo directo o indirecto, pudieran surgir de actos realizados al amparo del título habilitante concedido para el uso del dominio público radioeléctrico, con renuncia, en su caso, al fuero jurisdiccional extranjero que pudiera corresponder al solicitante.

Artículo 32. *Proyecto técnico y autorización para realizar la instalación de estaciones radioeléctricas en el caso de uso privativo del dominio público radioeléctrico sin limitación de número.*

A la solicitud de títulos habilitantes para uso privativo del dominio público radioeléctrico sin limitación de número, deberá acompañarse el correspondiente proyecto técnico, así como un estudio de emisiones radioeléctricas para aquellos casos en que resulte exigible de acuerdo con el artículo 53, salvo en los casos en que la presentación del proyecto pudiera presentarse con posterioridad a la obtención del título habilitante para el uso del dominio público radioeléctrico, según lo previsto en este reglamento.

Artículo 33. *Resolución del procedimiento.*

1. La Secretaría de Estado para la Sociedad de la Información y la Agenda Digital dictará resolución otorgando o denegando motivadamente el título solicitado, que se notificará al interesado en los términos previstos en el artículo 41 y siguientes de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. Dicha resolución pondrá fin a la vía administrativa.

2. Las resoluciones en virtud de las cuales se otorguen títulos habilitantes para el uso del dominio público radioeléctrico podrán incluir, cuando corresponda, la aprobación del proyecto técnico con las modificaciones que, en su caso, se hubieran determinado. La aprobación del proyecto técnico conlleva la autorización para realizar la instalación de las estaciones correspondientes. En dichas resoluciones se detallarán igualmente los parámetros técnicos de funcionamiento, incluyendo, cuando proceda, las coordenadas geográficas para cada una de las estaciones fijas, así como la potencia máxima de emisión de las mismas, los plazos de vigencia, la zona de servicio; la cuantificación de la tasa por reserva del dominio público radioeléctrico y el número de unidades de reserva radioeléctrica; los plazos para realizar las instalaciones y cualquier otra condición que deban cumplir sus titulares.

3. El plazo para resolver las solicitudes de otorgamiento, modificación y extinción de los títulos habilitantes para el uso del dominio público radioeléctrico será de seis semanas desde la fecha de entrada de la solicitud en la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital. Dicho plazo podrá suspenderse de acuerdo con lo previsto en el artículo 22 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

No obstante, de conformidad con lo dispuesto en el artículo 62.2 de la Ley General de Telecomunicaciones, no será de aplicación dicho plazo cuando sea necesaria la coordinación internacional de frecuencias o afecte a reservas de posiciones orbitales.

4. Transcurrido el plazo al que se refiere el apartado anterior sin haberse notificado resolución expresa, deberán entenderse desestimadas las solicitudes de otorgamiento y modificación de los títulos habilitantes para el uso del dominio público radioeléctrico, y estimadas las solicitudes de extinción de los títulos habilitantes para el uso del dominio público radioeléctrico, sin perjuicio de la obligación de la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital de resolver expresamente, de acuerdo con lo dispuesto en el artículo 24 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Artículo 34. *Denegación de solicitudes.*

La Secretaría de Estado para la Sociedad de la Información y la Agenda Digital podrá denegar las solicitudes de otorgamiento de títulos habilitantes para uso privativo del dominio público radioeléctrico por alguna de las siguientes causas:

a) Carecer de la condición de operador de comunicaciones electrónicas, en el caso de concesiones administrativas.

b) Incurrir en alguna de las prohibiciones de contratar reguladas en el texto refundido de la Ley de Contratos del Sector Público, aprobado mediante el Real Decreto Legislativo 3/2011, de 14 de noviembre, en el caso de concesiones administrativas.

c) No acreditar que el solicitante dispone o está en condiciones de obtener la capacidad de segmento espacial correspondiente a la red radioeléctrica que pretende instalar, proporcionada por el titular de la infraestructura satelital, en los casos de redes radioeléctricas que utilicen satélites.

d) No haber suficiente dominio público radioeléctrico disponible para el servicio solicitado en las bandas de frecuencia reservadas en el Cuadro Nacional de Atribución de Frecuencias.

e) Advertir que el número de interesados en la obtención de los derechos de uso es superior a la oferta disponible de dominio público radioeléctrico, o que se puedan producir situaciones de acaparamiento de espectro por parte de un mismo titular en determinadas bandas o subbandas de frecuencias.

f) Concurrir alguna de las causas para denegar la aprobación del proyecto técnico y la autorización para realizar la instalación a que hace referencia la sección 3.ª de este Capítulo.

Subsección 2.ª Uso privativo del dominio público radioeléctrico en una banda reservada

Artículo 35. *Concepto de banda reservada.*

1. La banda reservada de frecuencias constituye un caso particular de uso privativo del dominio público radioeléctrico sin limitación de número que permite la reserva en favor de un determinado titular de una banda o subbanda de frecuencias o de un conjunto de canales radioeléctricos para su utilización en una determinada zona geográfica. La banda reservada podrá ser objeto de uso compartido entre varios usuarios del mismo servicio de radiocomunicaciones.

Las reservas de banda están justificadas, por razones de eficacia en la gestión y uso del dominio público radioeléctrico, en casos de redes radioeléctricas que impliquen despliegues masivos de estaciones, destinadas a servicios que requieren disponer de grupos de frecuencias radioeléctricamente compatibles entre sí.

2. Mediante resolución del Secretario de Estado para la Sociedad de la Información y la Agenda Digital se identificarán las bandas de frecuencia que podrán ser explotadas bajo la modalidad de banda reservada.

Artículo 36. *Título habilitante para el uso del dominio público radioeléctrico en una banda reservada.*

El título habilitante para el uso de las bandas reservadas será el correspondiente al uso privativo del dominio público radioeléctrico sin limitación de número y el procedimiento para su obtención deberá ajustarse a lo indicado en la subsección 1.ª anterior, y en este reglamento.

Subsección 3.ª Uso privativo del dominio público radioeléctrico con limitación de número de titulares. Procedimiento de licitación

Artículo 37. *Título habilitante para el uso privativo del dominio público radioeléctrico con limitación de número de titulares, otorgado mediante el procedimiento de licitación.*

1. Cuando sea preciso para garantizar el uso eficaz o eficiente del dominio público radioeléctrico y en especial cuando la demanda de uso supere a la oferta, el Ministerio de

Energía, Turismo y Agenda Digital podrá limitar el número de concesiones a otorgar en determinadas bandas de frecuencias, de acuerdo con lo establecido en el artículo 63 de la Ley General de Telecomunicaciones.

2. A estos efectos, la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital realizará una consulta pública a fin de dar a todas las partes interesadas, incluidos los usuarios y consumidores, la oportunidad de manifestar su punto de vista sobre la posible limitación, y suspenderá el otorgamiento de títulos habilitantes para el uso del dominio público radioeléctrico en dichas bandas de frecuencias.

La Secretaría de Estado para la Sociedad de la Información y la Agenda Digital pondrá a disposición del público los resultados del procedimiento de consulta, salvo en el caso de información confidencial, y propondrá, en su caso, al Ministro de Energía, Turismo y Agenda Digital que incluya esas bandas de frecuencias dentro de la relación en la que el número de concesiones a otorgar queda limitado, a efecto de proceder al inicio de un procedimiento de licitación.

3. La relación inicial de bandas de frecuencias con limitación de títulos habilitantes para el uso del dominio público radioeléctrico a otorgar es la establecida en la disposición adicional primera de este reglamento.

4. El procedimiento de licitación no será de aplicación al otorgamiento de los recursos radioeléctricos cuando así lo requiera la aplicación de normas internacionales o convenios que obliguen al Reino de España.

5. Sin perjuicio de lo dispuesto en el Cuadro Nacional de Atribución de Frecuencias, en los pliegos reguladores de los procedimientos de licitación para el otorgamiento de títulos habilitantes para el uso del dominio público radioeléctrico se podrán establecer cautelas para promover la competencia en la prestación de los servicios, o para evitar comportamientos especulativos o acaparamiento de derechos de uso del dominio público radioeléctrico, en particular mediante la fijación de plazos estrictos para la explotación de los derechos de uso por parte de su titular, o la fijación de límites en la cantidad de frecuencias a utilizar por un mismo operador o grupo empresarial, incluidos los casos de cesión o mutualización de frecuencias.

6. Quienes resultasen seleccionados para la prestación de servicios de comunicaciones electrónicas armonizados en procedimientos de licitación convocados por las instituciones de la Unión Europea, en los que se establezca la reserva a su favor de derechos de uso del dominio público radioeléctrico, se inscribirán de oficio en el Registro de Operadores. La Secretaría de Estado para la Sociedad de la Información y la Agenda Digital otorgará de oficio, o a solicitud del interesado, la concesión a los operadores antes mencionados. En las citadas concesiones se incluirán, entre otras, las condiciones que proceda establecidas en los procedimientos de licitación, así como los compromisos adquiridos por el operador en dichos procedimientos.

Artículo 38. *Procedimiento de licitación.*

1. Mediante orden del Ministro de Energía, Turismo y Agenda Digital se aprobará la convocatoria y el pliego de bases del procedimiento de licitación para el otorgamiento de los títulos. En el citado pliego deberá establecerse:

a) La cantidad de dominio público reservada, las características de su utilización, el plazo de vigencia de los títulos y cualquier otra característica o condición para su uso efectivo.

b) El plazo para la presentación de las ofertas, que no podrá ser inferior a un mes.

c) Los requisitos y condiciones que hayan de cumplir los licitadores y los posibles adjudicatarios que, en su caso, deberán ostentar la condición de operador en el momento de finalización del plazo de presentación de solicitudes, y no incurrir en alguna de las prohibiciones de contratar reguladas en el texto refundido de la Ley de Contratos del Sector Público, aprobado mediante el Real Decreto Legislativo 3/2011, de 14 de noviembre.

d) Las posibles medidas para promover la competencia en la prestación de los servicios o evitar comportamientos especulativos o acaparamiento de derechos de uso del dominio público radioeléctrico, en particular estableciendo límites a la cantidad de espectro cuyos derechos de uso podrá ostentar un mismo titular.

e) La cuantía de la garantía provisional y la garantía definitiva cuya constitución pueda exigirse en función de la naturaleza de la red o del servicio.

f) Las condiciones en que deba prestarse el servicio o explotarse la red de comunicaciones electrónicas a que esté destinado el dominio público radioeléctrico reservado. En particular, se recogerá la posible obligación de que los adjudicatarios proporcionen oferta de servicios mayoristas de acuerdo con lo que establezca la normativa comunitaria.

2. El procedimiento de licitación, respetará en todo caso los principios de publicidad, concurrencia, no discriminación y transparencia.

3. Cuando en la adjudicación hayan de tenerse en cuenta criterios distintos del precio, podrán tenerse en cuenta, entre otros criterios de valoración según la naturaleza del servicio, los siguientes:

a) La cobertura y los plazos de despliegue de la red.

b) Las cantidades a destinar en inversión nueva.

c) El número de estaciones radioeléctricas a desplegar.

d) Las técnicas que permitan hacer un uso más eficaz y eficiente del dominio público radioeléctrico.

e) El compromiso voluntario de los licitadores de ofrecer el servicio a mayoristas.

4. La evaluación de los criterios de valoración y la propuesta de adjudicación se efectuará por una Mesa de Adjudicación.

La Mesa estará constituida por un Presidente, un mínimo de cinco Vocales y un Secretario.

Los miembros de la Mesa serán nombrados por el Ministro de Energía, Turismo y Agenda Digital. El Secretario, que actuará con voz pero sin voto, deberá ser designado entre funcionarios de la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital, y entre los Vocales deberán figurar un abogado del estado y un interventor o, a falta de estos, un funcionario de entre quienes tengan atribuido legal o reglamentariamente el asesoramiento jurídico al órgano de contratación y un funcionario que tenga atribuidas las funciones de control económico-presupuestario.

5. En todo lo no previsto en el pliego de bases en relación con la convocatoria, adjudicación, modificación, transmisión, cesión y extinción de los títulos otorgados mediante este procedimiento será de aplicación la legislación de Patrimonio de las Administraciones Públicas.

6. El procedimiento de licitación deberá resolverse mediante una orden del Ministro de Energía, Turismo y Agenda Digital y notificarse o publicarse en un plazo máximo de ocho meses desde la publicación de la convocatoria.

7. Las condiciones en que deba prestarse el servicio o explotarse la red serán las previstas en la Ley General de Telecomunicaciones y su normativa de desarrollo, las específicas establecidas en el pliego de bases y las que el licitador, en su caso, haya asumido en su propuesta.

8. La relación de bandas de frecuencia con limitación del número de títulos habilitantes de uso del dominio público radioeléctrico podrá ser revisada por el Ministerio de Energía, Turismo y Agenda Digital, de oficio o a instancia de parte, previo informe preceptivo de la Comisión Nacional de los Mercados y la Competencia, y previo acuerdo de la Comisión Delegada del Gobierno para Asuntos Económicos. En caso de efectuarse dicha revisión, no habrá derecho a indemnización a favor de los titulares que hubieran obtenido sus concesiones mediante el procedimiento de licitación, sin perjuicio del derecho de los mismos a la cancelación de las garantías que, en su caso, hubiesen constituido para responder de compromisos asumidos en el procedimiento.

9. En el caso de concesiones para el uso privativo del dominio público radioeléctrico otorgadas por un procedimiento de licitación, las competencias sobre renovación, modificación, extinción, revocación, cesión y transferencia del título, así como sobre mutualización de derechos de uso y provisión de servicios mayoristas relevantes, corresponden al Ministro de Energía, Turismo y Agenda Digital.

Subsección 4.ª Uso privativo del dominio público radioeléctrico para la prestación de servicios de radiodifusión sonora y de televisión

Artículo 39. *Título habilitante para el uso del dominio público radioeléctrico para la prestación de servicios de radiodifusión sonora y de televisión por ondas terrestres.*

1. Para los supuestos de prestación de servicios de radiodifusión sonora y de televisión por ondas terrestres, el derecho de uso de dominio público radioeléctrico se otorgará, de conformidad con lo previsto en los planes técnicos nacionales, por la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital mediante concesión administrativa aneja al título habilitante audiovisual.

2. Los órganos del Estado y de las Comunidades Autónomas competentes para el otorgamiento de títulos habilitantes audiovisuales para la prestación de servicios de radiodifusión sonora y de televisión por ondas terrestres, deberán comunicar a la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital los títulos otorgados, así como sus eventuales modificaciones, incluyendo las posibles condiciones asociadas a los mismos, así como los datos de los titulares de cada uno de los títulos concedidos, en el plazo de quince días contados desde la fecha su otorgamiento. Asimismo, deberán comunicar a la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital, en dicho plazo, la extinción de los títulos habilitantes audiovisuales.

Las concesiones del dominio público radioeléctrico para la prestación de los citados servicios de radiodifusión sonora y de televisión por ondas terrestres se otorgarán y, en su caso, se modificarán o extinguirán de oficio por la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital, una vez recibida la comunicación señalada en el párrafo anterior, y serán notificados a los titulares del título audiovisual correspondiente.

La Secretaría de Estado para la Sociedad de la Información y la Agenda Digital informará a los órganos competentes del Estado y de las Comunidades Autónomas sobre las concesiones para el uso del dominio público radioeléctrico aparejadas a los títulos audiovisuales otorgados por ellos en el plazo de quince días, contados desde la fecha de otorgamiento.

3. Una vez obtenida la concesión de dominio público radioeléctrico para la prestación de los citados servicios de radiodifusión sonora y de televisión por ondas terrestres, el titular deberá presentar ante la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital el oportuno proyecto técnico de la estación o estaciones a instalar. Dicha solicitud se tramitará conforme a lo señalado en la sección 3.ª del presente capítulo.

4. La autorización de los negocios jurídicos de transmisión o arrendamiento sobre licencias de comunicación audiovisual por los órganos del Estado o de las Comunidades Autónomas, competentes en material audiovisual, requerirá con carácter previo la autorización por la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital en lo referente a la transmisión o cesión de la concesión de dominio público radioeléctrico anejo al título habilitante audiovisual, en los términos previstos en el Título VI de este reglamento.

Subsección 5.ª De los recursos órbita-espectro

Artículo 40. *Recursos órbita-espectro: Concepto y naturaleza.*

1. Son recursos órbita-espectro, a los efectos de este reglamento, aquellos necesarios para soportar una infraestructura satelital de radiocomunicaciones constituida por cada una de las posiciones de la órbita geoestacionaria o bien un conjunto de órbitas no geoestacionarias susceptibles de albergar un sistema de satélites, las zonas de servicio y las frecuencias pre-coordinadas de servicios espaciales.

2. La utilización de los derechos del Reino de España sobre los recursos órbita-espectro estará sometida al derecho internacional y, en particular, a lo dispuesto en los Tratados de la Constitución, Convenio y Reglamento de Radiocomunicaciones de la Unión Internacional de Telecomunicaciones (UIT).

Las relaciones del Reino de España con la UIT para tramitar las reservas de recursos órbita-espectro a favor del Reino de España están excluidas de la regulación de este

reglamento, que tiene por objeto las relaciones entre la Administración española y los interesados en la obtención a su favor de los derechos de uso sobre dichos recursos.

3. La utilización del dominio público radioeléctrico necesaria para la utilización de los recursos órbita-espectro en el ámbito de la soberanía española y mediante satélites de comunicaciones queda reservada al Estado. Su explotación estará sometida al derecho internacional y se realizará mediante su gestión directa por el Estado o mediante concesión otorgada por la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital. La gestión de los recursos órbita-espectro podrá también llevarse a cabo mediante conciertos con organismos internacionales.

4. El derecho de uso de recursos órbita-espectro en el ámbito de la soberanía española tendrá la consideración de derecho de uso privativo de dominio público radioeléctrico y le será de aplicación, además de lo previsto en este reglamento, lo establecido en la Ley General de Telecomunicaciones y sus normas de desarrollo.

Artículo 41. *Título habilitante para el uso privativo de recursos órbita-espectro.*

1. Los derechos de uso de los recursos órbita-espectro, que hayan sido otorgados a un organismo del Estado para la prestación de los servicios que tenga encomendados, podrán ser utilizados por ésta mediante gestión directa o indirecta, de conformidad con lo establecido en su normativa específica.

2. Los derechos de uso de los recursos órbita-espectro cuya gestión no sea realizada de manera directa por el Estado se obtendrán mediante concesión administrativa en los términos previstos en este reglamento.

3. Una vez publicada por la UIT la información relativa a la solicitud de reserva del recurso órbita-espectro presentada por el Reino de España, se podrá otorgar una autorización provisional para la explotación de dicho recurso, si se reúnen todas las condiciones requeridas para dicha explotación. En todo caso, dicha autorización estará condicionada por las características técnicas y limitaciones derivadas del proceso de coordinación internacional y podrá ser cancelada si existen condicionantes técnicos que impidan la correcta explotación del recurso órbita-espectro o si, finalmente, la UIT no concede la reserva del recurso orbita-espectro a favor del Reino de España.

4. En el caso de que la infraestructura satelital de radiocomunicaciones incluya una red terrenal subordinada, las frecuencias de dicha red terrenal, distintas de las frecuencias pre-coordinadas de servicios espaciales, no estarán incluidas en el título habilitante para el uso privativo del recurso órbita-espectro, siendo necesaria la obtención del correspondiente título habilitante para el uso privativo de dicho dominio público radioeléctrico.

Artículo 42. *Procedimiento de obtención del título habilitante para el uso privativo de recursos órbita-espectro.*

1. A las solicitudes de otorgamiento de título habilitante para el uso privativo de los recursos órbita-espectro les será de aplicación lo establecido en la subsección 1.ª anterior, sin perjuicio de las condiciones específicas enumeradas en esta subsección.

2. El interesado se hará cargo directamente, y a su costa, de cualquier obligación económica que genere la UIT en relación con el procedimiento de reserva del recurso órbita-espectro.

A tal efecto, en el caso de que el título habilitante solicitado para el uso del recurso órbita-espectro fuera una concesión administrativa, la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital, antes de dictar la resolución sobre el otorgamiento del mismo, exigirá la constitución al interesado de una garantía destinada a asegurar el cumplimiento del compromiso de hacer frente a cualquier obligación económica que genere la UIT en relación con el procedimiento de reserva del recurso órbita-espectro.

Como norma general, la cuantía de la garantía a la que hace referencia el párrafo anterior será de 200.000 euros. No obstante, podrán exigirse garantías inferiores en función de la simplicidad del procedimiento a desarrollar.

La garantía deberá constituirse y depositarse en la Caja General de Depósitos, en los términos establecidos en el Real Decreto 161/1997, de 7 de febrero, que aprueba el Reglamento de la Caja General de Depósitos, en el plazo de un mes a contar desde el

requerimiento efectuado, al efecto, por la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital.

3. La Secretaría de Estado para la Sociedad de la Información y la Agenda Digital, antes de dictar la resolución sobre el otorgamiento o denegación del título habilitante necesario para el uso del recurso órbita-espectro, podrá requerir al solicitante cuanta información, estudios o aclaraciones considere convenientes sobre su solicitud o sobre los documentos con ella presentados. En concreto, podrá requerir cuantos datos y documentos adicionales considere necesarios para evaluar la solvencia económica y técnica del solicitante, así como la viabilidad del proyecto.

El solicitante está obligado, a su costa, para aportar a la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital la información, estudios o aclaraciones que le haya requerido. En caso de que el solicitante no aporte la información, estudios o aclaraciones requeridos, o bien los mismos sean insuficientes para continuar con el normal desarrollo del procedimiento de reconocimiento por la UIT de la reserva del recurso órbita-espectro, y posterior otorgamiento del título habilitante para el uso de dicho recurso, la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital dictará resolución por la que se le tendrá por desistido de su solicitud.

4. El plazo de que dispone la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital, para resolver las solicitudes de otorgamiento de títulos habilitantes para el uso privativo de recursos órbita-espectro, será de seis semanas a contar desde que la UIT haya reconocido la reserva del recurso órbita-espectro a favor del Reino de España.

5. Transcurrido el plazo al que se refiere el apartado anterior sin haberse notificado resolución expresa, deberán entenderse desestimadas las solicitudes, sin perjuicio de la obligación de la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital de resolver expresamente, de acuerdo con lo dispuesto en el artículo 24 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Artículo 43. *Documentación adicional.*

La solicitud de título habilitante para el uso privativo de los recursos órbita-espectro deberá ir acompañada de la documentación siguiente:

1. Características técnicas de la red o sistema de satélites así como de los servicios de comunicaciones por satélite a ofrecer, cobertura prevista, calidad de la señal, balances de los distintos enlaces, entre otros, así como su adecuación a la normativa en vigor y al Reglamento de Radiocomunicaciones de la UIT.

2. Declaración del material, instalaciones y equipo técnico que tenga previsto utilizar en la ejecución del proyecto.

3. Presupuesto económico desglosado y total estimado para la ejecución íntegra del proyecto, incluyendo el segmento espacial y el segmento terreno, así como los costes de lanzamiento y seguros.

4. Compromiso de que los centros de gestión y estaciones de control del sistema de satélites estarán radicados en España, siempre y cuando sea técnicamente posible.

5. Documentación que permita acreditar la solvencia económica y técnica del solicitante, mediante la presentación de los siguientes documentos:

a) Balances o extractos de balances del último ejercicio económico, debidamente auditados.

b) Declaración relativa a la cifra de negocios global en los últimos tres ejercicios.

c) Relación de los principales servicios o trabajos realizados en los últimos tres años que incluya importe, fechas y beneficiarios públicos o privados de los mismos.

d) Declaración que indique el promedio anual de personal y plantilla de directivos durante los tres últimos años.

e) Declaración de las medidas adoptadas por los empresarios para controlar la calidad, así como de los medios de estudio y de investigación de que dispongan.

f) Cualificación de los cuadros técnicos relacionados con el proyecto.

Artículo 44. *Denegación de solicitudes.*

La Secretaría de Estado para la Sociedad de la Información y la Agenda Digital podrá denegar mediante resolución motivada las solicitudes, además de por alguna de las causas mencionadas en el artículo 34, por las siguientes:

a) Falta de solvencia económica o técnica del solicitante o falta de viabilidad del proyecto.

b) Razones de interés público, de fomento de competencia en los mercados de redes y servicios de comunicaciones electrónicas, o de desarrollo del sector de las telecomunicaciones y de la Sociedad de la Información, debidamente acreditadas.

Artículo 45. *Obligaciones específicas de los titulares de los derechos de uso privativo de recursos órbita-espectro.*

Además de lo establecido en los títulos III, V y VI, son obligaciones específicas de los titulares de los derechos de uso de recursos órbita-espectro las siguientes:

a) Cuando a través de dichos recursos órbita-espectro se presten servicios de difusión, el titular de los derechos de uso del recurso órbita-espectro estará obligado a notificar a la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital el servicio o servicios concretos que se prestan y el título habilitante de difusión al amparo del cual se proveen los servicios.

b) Abstenerse de facilitar el uso del recurso órbita-espectro a los usuarios que carezcan o les haya sido revocado el título para la prestación de servicios de difusión o de comunicaciones electrónicas, según proceda, o que carezcan o les haya sido revocado el título habilitante de derechos de uso de dominio público radioeléctrico para su explotación en redes de comunicaciones electrónicas que utilicen los recursos órbita-espectro.

Artículo 46. *Derechos de gratuidad en los procedimientos de obtención de recursos órbita-espectro ante la UIT.*

El Reino de España, como Estado Miembro de la UIT, con carácter anual, tiene el derecho de gratuidad sobre la unidad más simple de recursos orbitales definida como «red de satélite» por la UIT, de acuerdo con su normativa.

Para la selección de la red susceptible de aplicación del procedimiento de gratuidad, se aplicarán los siguientes criterios conforme al siguiente orden de prelación:

a) Redes de satélite cuyo operador sea una Administración Pública, frente a otras posibles redes.

b) Red que suponga el coste más elevado, siempre que sea compatible con las decisiones del Consejo de la UIT.

Subsección 6.ª Uso privativo del dominio público radioeléctrico para fines experimentales y eventos de corta duración.

Artículo 47. *Concepto.*

El uso privativo del dominio público radioeléctrico para fines experimentales y eventos de corta duración constituye un caso particular de uso privativo del dominio público radioeléctrico sin limitación de número.

A los efectos de este reglamento, tendrán la consideración de usos experimentales los destinados a efectuar pruebas técnicas o ensayos sobre propagación, utilización de nuevas bandas de frecuencia o demostraciones de nuevos servicios o tecnologías. Los eventos de corta duración incluirán los acontecimientos deportivos, culturales u otros de especial interés.

Artículo 48. *Título habilitante para el uso privativo del dominio público radioeléctrico para fines experimentales y eventos de corta duración.*

1. El otorgamiento del título habilitante para el uso del dominio público radioeléctrico para eventos de corta duración y para usos experimentales se regirá por lo establecido en la subsección 1.ª anterior, con las condiciones específicas señaladas en el presente artículo.

2. A la solicitud del título habilitante para el uso del dominio público radioeléctrico y de autorización para realizar la instalación, deberá acompañarse una memoria técnica que incluirá una descripción del servicio a prestar, la red radioeléctrica, las estaciones y los equipos que se pretenden utilizar, con indicación de sus características técnicas y ubicación, y el período de utilización.

3. La solicitud de título habilitante para el uso del dominio público radioeléctrico para la cobertura de eventos de corta duración o para fines experimentales se presentará ante la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital con una antelación de, al menos, diez días hábiles al comienzo del período de utilización solicitado.

Sección 3.ª Instalación de estaciones radioeléctricas destinadas al uso privativo del dominio público radioeléctrico

Artículo 49. *Procedimiento para aprobación del proyecto técnico y para autorizar la instalación de estaciones radioeléctricas fijas.*

1. Para realizar la instalación de una estación radioeléctrica fija o una red de estaciones fijas, el interesado deberá presentar ante la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital un proyecto técnico, que incluirá el correspondiente estudio de emisiones radioeléctricas, para aquellos casos en que resulte exigible.

El proyecto técnico, y el estudio de emisiones radioeléctricas se ajustarán a lo señalado en la presente sección.

2. Con carácter general, el proyecto técnico se presentará conjuntamente con la solicitud del correspondiente título habilitante para el uso privativo del dominio público radioeléctrico. En dicho caso, la resolución de otorgamiento del título habilitante para el uso del dominio público radioeléctrico incluirá la aprobación del proyecto técnico. La aprobación del proyecto técnico conllevará la autorización para realizar la instalación de las estaciones radioeléctricas correspondientes.

3. La presentación del proyecto técnico podrá realizarse con posterioridad al otorgamiento del correspondiente título habilitante para el uso del dominio público radioeléctrico en los casos siguientes:

c) Uso privativo del dominio público radioeléctrico en el caso de banda reservada.

d) Uso privativo del dominio público radioeléctrico con limitación de número otorgado mediante el procedimiento de licitación.

e) Uso privativo del dominio público radioeléctrico para la prestación de servicios de radiodifusión sonora y de televisión.

f) Cuando así se autorice en la resolución de otorgamiento del correspondiente título habilitante para el uso del dominio público radioeléctrico, previa petición motivada del solicitante, en particular en los casos de grandes redes de estaciones radioeléctricas, cuyo despliegue se produzca de manera progresiva.

El interesado acompañará a su solicitud un documento que acredite su personalidad y la identificación del título habilitante para el uso del dominio público radioeléctrico a que se refiere la misma, además de la documentación técnica correspondiente.

4. Cuando sea preciso para garantizar una gestión eficaz y eficiente del dominio público radioeléctrico, la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital podrá proponer la modificación del proyecto técnico presentado, manteniendo los objetivos de servicio propuestos por el solicitante o, en su caso, previstos en el título habilitante para el uso del dominio público radioeléctrico.

5. La Secretaría de Estado para la Sociedad de la Información y la Agenda Digital dictará resolución aprobando el proyecto técnico con las modificaciones que, en su caso, se hubieran determinado y concediendo la autorización para realizar la instalación correspondiente, o denegando motivadamente la solicitud.

Dicha resolución se notificará al interesado, en los términos previstos en el artículo 41 y siguientes de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y pondrá fin a la vía administrativa.

6. En dichas resoluciones, cuando proceda aprobar el proyecto técnico y autorizar la realización de la instalación, se detallarán los parámetros técnicos de funcionamiento,

incluyendo las coordenadas geográficas para cada una de las estaciones fijas, así como la potencia máxima de emisión de las mismas, la zona de servicio; los plazos para realizar las instalaciones y para solicitar la autorización para la puesta en servicio, así como cualquier otra condición que deban cumplir sus titulares.

7. El plazo para resolver las solicitudes será de seis semanas desde la fecha de entrada de la solicitud en la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital. En el caso de proyectos técnicos para el uso privativo del dominio público radioeléctrico para la prestación de servicios de radiodifusión sonora y de televisión dicho plazo será el establecido en los correspondientes Planes Técnicos Nacionales o, en su defecto, de seis meses. El plazo podrá suspenderse de acuerdo con lo previsto en el artículo 22 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

No obstante, de conformidad con lo dispuesto en el artículo 62.2 de la Ley General de Telecomunicaciones, no serán de aplicación dichos plazos cuando sea necesaria la coordinación internacional de frecuencias.

8. Transcurridos los plazos a los que se refiere el apartado anterior sin haberse notificado resolución expresa, deberán entenderse desestimadas las solicitudes, sin perjuicio de la obligación de la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital de resolver expresamente, de acuerdo con lo dispuesto en el artículo 24 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

9. La aprobación del proyecto técnico y la autorización para realizar la instalación es el título que habilita a su titular para realizar la instalación, y para emitir en pruebas por el tiempo indispensable para poder comprobar que el funcionamiento de la instalación radioeléctrica realizada es el adecuado. Dichas emisiones en pruebas se limitarán al periodo de tiempo durante el cual se estén realizando de forma material las medidas y comprobaciones técnicas pertinentes, y, en ningún caso, habilitan al titular para la utilización del dominio público radioeléctrico.

10. La aprobación del proyecto técnico y de la correspondiente autorización para realizar la instalación de estaciones radioeléctricas estará condicionada a que, en el plazo de nueve meses, el titular realice la instalación de la estación y comunique a la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital la finalización de la misma, solicitando la autorización para su puesta en servicio, conforme a lo previsto en este reglamento. No obstante, de manera excepcional, podrá autorizarse en la resolución de aprobación del proyecto técnico un plazo superior, en aquellos casos en los que la complejidad de la red de estaciones así lo requiera.

Transcurrido dicho plazo sin haber cumplido lo señalado en el párrafo anterior o cuando se deniega la autorización de puesta en servicio, quedará sin efecto la aprobación del proyecto y la correspondiente autorización para realizar la instalación, y se procederá a su archivo sin más trámite.

Artículo 50. *Denegación de solicitudes.*

La Secretaría de Estado para la Sociedad de la Información y la Agenda Digital podrá denegar la aprobación del proyecto técnico y la autorización para realizar las instalaciones por alguna de las siguientes causas:

a) No adecuarse las características técnicas de la red que se pretende instalar a los planes de utilización del dominio público o al Cuadro Nacional de Atribución de Frecuencias.

b) No aceptar las modificaciones de las características técnicas del proyecto técnico que hubieran sido propuestas por la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital.

c) No garantizar las características de la red que se pretende instalar un uso eficaz y eficiente del dominio público radioeléctrico, o exista falta de adecuación entre las necesidades de radiocomunicaciones planteadas y el uso del dominio público radioeléctrico que se solicita.

Artículo 51. *Procedimiento simplificado para aprobación del proyecto técnico y autorización para realizar la instalación de estaciones radioeléctricas fijas.*

1. La aprobación del proyecto técnico y la correspondiente autorización para realizar la instalación de estaciones podrá realizarse a través del procedimiento simplificado previsto en el presente artículo en los casos siguientes:

a) Uso privativo del dominio público radioeléctrico con limitación de número otorgado mediante el procedimiento de licitación, para aquellos tipos de estaciones que se determinen mediante resolución del Secretario de Estado para la Sociedad de la Información y la Agenda Digital.

b) Uso privativo del dominio público radioeléctrico en el caso de banda reservada, para las estaciones en que se hubiera previsto en la resolución de otorgamiento del correspondiente título habilitante para el uso del dominio público radioeléctrico.

c) En aquellas bandas de frecuencia, servicios o tipos de estaciones que se determinen mediante resolución del Secretario de Estado para la Sociedad de la Información y la Agenda Digital, atendiendo al tipo de servicio a prestar o por presentar las estaciones características técnicas similares.

d) Cuando así se autorice en la resolución de otorgamiento del correspondiente título habilitante para el uso del dominio público radioeléctrico, previa petición motivada del solicitante, en aquellos casos en los que se trate de redes de estaciones de características técnicas similares.

2. Los titulares presentarán ante la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital, para su aprobación, un proyecto técnico tipo para cada una de las categorías o clases de estaciones que pretendan instalar. La aprobación del proyecto técnico tipo se realizará conforme a lo previsto en el artículo 49.

3. En los casos de redes radioeléctricas incluidas en los casos previstos en los epígrafes a), b) y c) del apartado 1 de este artículo, cuyas estaciones presenten características técnicas similares, la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital podrá establecer las características técnicas tipo de las estaciones radioeléctricas correspondientes.

4. Una vez aprobado el proyecto tipo, o las características técnicas tipo señaladas en el apartado anterior, los titulares presentarán ante la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital, con carácter previo a su instalación, una declaración responsable con la relación de las estaciones que pretenden instalar, firmada por un técnico competente en materia de telecomunicaciones, en la que se indicará el proyecto técnico tipo o las características técnicas tipo a que se ajusta cada estación y los parámetros técnicos específicos de cada una de ellas, así como el estudio previo de niveles de exposición radioeléctrica de cada una de las estaciones, cuando sea preceptivo.

La notificación a la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital de la citada declaración responsable, habilitará al titular para realizar la instalación de las estaciones correspondientes, salvo que se constate que la declaración no reúne los requisitos necesarios. En este caso, la citada Secretaría de Estado dictará resolución motivada dejando sin efecto la habilitación para realizar la citada instalación.

5. En el caso de estaciones radioeléctricas con potencia isotrópica radiada equivalente igual o inferior a 1 vatio, la aprobación del proyecto técnico tipo constituirá condición suficiente para realizar la instalación y para la puesta en servicio de las estaciones correspondientes. En este caso, en el plazo de quince días desde que las estaciones se hayan instalado, el titular remitirá a la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital una declaración responsable con la relación de estaciones instaladas, indicando la ubicación y tipo de estación, y manifestando que las estaciones instaladas son conformes con el proyecto técnico tipo aprobado, excepto en los supuestos previstos en el apartado 1 de este artículo, en los que esta declaración se enviará bimestralmente. Igualmente, el titular remitirá en el plazo de quince días una declaración responsable cuando las estaciones hayan sido canceladas.

6. La Secretaría de Estado para la Sociedad de la Información y la Agenda Digital podrá exigir en cualquier momento la presentación de un proyecto técnico correspondiente a

cualquiera de las estaciones radioeléctricas incluidas en las declaraciones responsables señaladas en los apartados anteriores.

7. Mediante resolución del Secretario de Estado para la Sociedad de la Información y la Agenda Digital podrán establecerse modelos y contenido a los que habrán de ajustarse los citados proyectos técnicos tipo, así como el contenido de las declaraciones responsables señaladas en el presente artículo.

Artículo 52. *Proyecto técnico.*

1. El proyecto técnico describirá con precisión el servicio al que se pretende destinar la instalación de estaciones radioeléctricas, la solución técnica adaptada a las necesidades de radiocomunicaciones planteadas que permita justificar el uso del dominio público radioeléctrico que se solicita, incluirá la tipología de la estación o estaciones fijas proyectadas conforme a la clasificación establecida por la Orden CTE/23/2002, de 11 de enero, indicará el propietario o responsable de las mismas y será firmado por un técnico competente en materia de telecomunicaciones.

2. En el proyecto técnico se especificarán con el nivel de detalle necesario las características técnicas de la estación radioeléctrica o red de estaciones que presten el mismo servicio y pertenezcan a la misma red que se pretende instalar, incluyendo cuando corresponda las coordenadas geográficas, la potencia máxima de emisión, la frecuencia y la tipología de cada estación fija y su zona de servicio, así como los planos topográficos de escala adecuada, y cuanta otra información sea necesaria para la descripción técnica de la red radioeléctrica.

3. Deberá elaborarse igualmente un proyecto cuando, una vez obtenido el título habilitante para el uso del dominio público radioeléctrico, se solicite cualquier modificación de la composición o de los parámetros técnicos de la red radioeléctrica autorizada, incluyendo la instalación de nuevas estaciones o la cancelación de alguna de ellas. En el caso de que la cancelación se refiera a todas las estaciones que se reflejan en el proyecto técnico, bastará con una comunicación del titular a la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital para cancelarlas.

4. Mediante resolución del Secretario de Estado para la Sociedad de la Información y la Agenda Digital podrán aprobarse modelos y contenido a los que habrá de ajustarse el proyecto técnico, para los diferentes tipos de servicios de radiocomunicaciones o redes radioeléctricas.

Artículo 53. *Estudio previo de niveles de exposición radioeléctrica.*

1. El proyecto técnico de las estaciones fijas, con potencia isotrópica radiada equivalente máxima superior a 10 vatios, deberá incorporar un estudio detallado, realizado por un técnico competente, que indique los niveles de exposición radioeléctrica en áreas cercanas a sus instalaciones que se encuentren en entorno urbano o donde puedan permanecer habitualmente personas, en los casos de redes públicas de comunicaciones que presten los siguientes servicios:

a) Servicios de radiodifusión sonora y televisión.

b) Servicios de comunicaciones electrónicas en las bandas de frecuencias con limitación de número de títulos a otorgar identificadas en la disposición adicional primera de este reglamento.

c) Servicio de radiobúsqueda.

d) Servicio de comunicaciones móviles en grupo cerrado de usuarios.

e) Servicio fijo por satélite, servicio móvil por satélite y servicio de radiodifusión por satélite.

f) Servicios de acceso inalámbrico fijo y servicio fijo punto a multipunto, distintos a los contemplados en el anterior apartado b).

Los mencionados niveles de exposición, valorados teniendo en cuenta el entorno radioeléctrico, deberán cumplir los límites establecidos en el anexo II del Reglamento que establece condiciones de protección del dominio público radioeléctrico, restricciones a las emisiones radioeléctricas y medidas de protección sanitaria frente a emisiones radioeléctricas, aprobado por el Real Decreto 1066/2001, de 28 de septiembre.

2. El estudio de niveles de exposición radioeléctrica mostrará la exposición simultánea de los campos emitidos por todas las posibles estaciones radioeléctricas que influyan en cada uno de los puntos de medida, bien provengan de estaciones que presten servicios del mismo titular de derechos de uso del dominio público radioeléctrico o de titulares diferentes.

3. Para realizar dicho estudio, el técnico competente en materia de telecomunicaciones tomará medidas, al menos, en cinco puntos cercanos a la estación radioeléctrica fija que se quiere instalar y, sobre ellas, se calculará el nivel que existiría al poner en servicio la futura estación. Mediante resolución del Secretario de Estado para la Sociedad de la Información y la Agenda Digital podrán establecerse los criterios para la elección de dichos puntos.

Las medidas se realizarán según el procedimiento previsto en la Orden CTE/23/2002, de 11 de enero, por la que se establecen condiciones para la presentación de determinados estudios y certificaciones por operadores de servicios de radiocomunicaciones.

La Secretaría de Estado para la Sociedad de la Información y la Agenda Digital podrá exigir, en cualquier momento, la presentación del resultado de las medidas o cualquier otra documentación relacionada con el cumplimiento de los límites de exposición a las emisiones radioeléctricas.

El certificado de calibración de los equipos de medida se incorporará como anexo al citado estudio.

4. El estudio mostrará el correspondiente volumen de referencia, teniendo en cuenta las estaciones preexistentes en el entorno de la estación que pudieran influir en su cálculo, de manera que, en el exterior de dicho volumen, no se superen los límites establecidos en el anexo II del reglamento aprobado mediante el Real Decreto 1066/2001, de 28 de septiembre.

5. En la planificación de todas las instalaciones radioeléctricas, los titulares deberán tener en consideración, entre otros criterios, los siguientes:

a) La ubicación, características y condiciones de funcionamiento de las estaciones radioeléctricas deben minimizar los niveles de exposición del público en general a las emisiones radioeléctricas con origen tanto en éstas como, en su caso, en los terminales asociados a las mismas, manteniendo una adecuada calidad del servicio.

b) En el caso de instalación de estaciones radioeléctricas en cubiertas de edificios residenciales, los titulares de instalaciones radioeléctricas procurarán, siempre que sea posible, instalar el sistema emisor de manera que el diagrama de emisión no incida sobre el propio edificio, terraza o ático, ni sobre los colindantes.

c) La compartición de emplazamientos podría estar condicionada por la consiguiente concentración de emisiones radioeléctricas. Los operadores que compartan un mismo emplazamiento se facilitarán mutuamente, o a través del gestor del emplazamiento, los datos técnicos necesarios para realizar el estudio de que el conjunto de las instalaciones no supera los límites de exposición radioeléctrica.

d) De manera particular, la ubicación, características y condiciones de funcionamiento de las estaciones radioeléctricas debe minimizar, en la mayor medida posible, los niveles de emisión sobre espacios considerados sensibles.

6. En el caso de estaciones con potencia isotrópica radiada equivalente máxima superior a 10 vatios, se deberá especificar en el proyecto técnico la señalización de la estación radioeléctrica, conforme a las normas técnicas sobre señales de seguridad y, adicionalmente, cuando sea exigible, se especificará el vallado que restrinja el acceso de personal no profesional en instalación, mantenimiento o inspección de estaciones radioeléctricas, a zonas en las que pudieran superarse los límites establecidos en el anexo II del reglamento aprobado mediante el Real Decreto 1066/2001, de 28 de septiembre, cuando no existan otros elementos que lo puedan impedir. En este caso, el vallado o sistema equivalente deberá incorporar también la señalización de prohibición de acceso al personal no profesional en instalación, mantenimiento o inspección de estaciones radioeléctricas.

7. No podrán establecerse nuevas instalaciones radioeléctricas o modificarse las existentes cuando su funcionamiento pudiera suponer que se superen los límites establecidos en el anexo II del reglamento aprobado mediante el Real Decreto 1066/2001, de 28 de septiembre.

8. La validez del estudio de los niveles de exposición será de tres meses, desde el momento en el que se realiza la medición hasta que se presenta el proyecto técnico en la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital.

9. El Ministerio de Energía, Turismo y Agenda Digital podrá ampliar las obligaciones previstas en los apartados anteriores a otras instalaciones radioeléctricas.

10. Mediante resolución del Secretario de Estado para la Sociedad de la Información y la Agenda Digital podrán aprobarse modelos y contenido a los que habrá de ajustarse el estudio previo de emisiones radioeléctricas a que se refiere este artículo.

11. El Ministerio de Sanidad, Servicios Sociales e Igualdad tendrá acceso a la información que le resulte necesaria sobre los niveles de exposición a los que se refiere este artículo. Las autoridades sanitarias de las Comunidades Autónomas serán informadas por dicho Ministerio cuando lo soliciten.

TÍTULO IV

Puesta en servicio de las estaciones radioeléctricas

Artículo 54. *Autorización para la puesta en servicio de estaciones.*

1. Los titulares de derechos de uso del dominio público radioeléctrico a los que se hubiera aprobado el proyecto técnico y autorizado para realizar la correspondiente instalación de una nueva estación fija o una modificación de una estación existente, deberán obtener de la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital la autorización para la puesta en servicio de la estación una vez finalizada su instalación.

La autorización para la puesta en servicio de una determinada estación faculta a su titular a la utilización del dominio público radioeléctrico para dicha estación, y será concedida una vez que se haya procedido a la inspección o el reconocimiento técnico satisfactorio de las instalaciones, y se haya comprobado que se ajustan a las condiciones y características previamente autorizadas.

En el caso de que se haya autorizado una modificación que no implique el uso de nuevos recursos del dominio público radioeléctrico, en particular el cese en la utilización de una o varias frecuencias o estaciones, no será necesario solicitar la autorización para la puesta en servicio de las estaciones afectadas.

2. En el caso de las redes radioeléctricas que conlleven la utilización de estaciones portátiles o móviles, el título habilitante para el uso del dominio público radioeléctrico habilita para la puesta en servicio de las citadas estaciones, siempre que cumplan con la normativa vigente.

3. Se considerará autorizada, con carácter general, la puesta en servicio de las estaciones radioeléctricas destinadas al uso común del dominio público radioeléctrico, siempre que cumplan con la normativa vigente.

4. Asimismo, se considerará autorizada, con carácter general, la puesta en servicio de estaciones radioeléctricas con potencia isotrópica radiada equivalente igual o inferior a 1 vatio, siempre que cumplan las condiciones señaladas en el apartado 5 del artículo 51, y con la normativa vigente.

5. La autorización para la puesta en servicio de estaciones correspondientes al uso especial del dominio público radioeléctrico, tanto en el caso de autorización general como de autorización individual, se regirá por lo establecido en la normativa específica que regule este tipo de uso.

6. La autorización para la puesta en servicio de estaciones correspondientes al uso privativo del dominio público, se regirá por lo establecido en el presente Título. En el caso de estaciones destinadas a eventos de corta duración se considerará autorizada la puesta en servicio en las condiciones técnicas que se hubieran establecido en el correspondiente título habilitante para el uso del dominio público radioeléctrico.

Artículo 55. *Reconocimiento técnico de las instalaciones previo a la autorización para la puesta en servicio.*

1. Antes de autorizar la puesta en servicio de una estación, y con el fin de comprobar que las instalaciones se ajustan a las condiciones previamente autorizadas, la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital realizará un reconocimiento técnico de la instalación, de acuerdo con lo previsto en el artículo 62.9 de la Ley General de Telecomunicaciones.

2. El reconocimiento técnico de las instalaciones se realizará una vez que el titular de los derechos de uso del dominio público radioeléctrico haya presentado la solicitud de autorización para la puesta en servicio ante la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital. En dicha solicitud se identificará tanto al propietario de las instalaciones como al operador que efectúa materialmente las emisiones radioeléctricas, en caso de que éstos no fueran el titular de los derechos de uso. Para poder realizar el citado reconocimiento, y únicamente durante el tiempo en que se produzcan las actuaciones técnicas de inspección, la estación podrá funcionar en pruebas.

3. Dicho reconocimiento técnico de las instalaciones será sustituido por una certificación de instalación de la estación radioeléctrica, firmada por técnico competente en materia de telecomunicaciones, en los casos previstos en este reglamento.

4. Para obtener la autorización para la puesta en servicio será preceptivo obtener un reconocimiento técnico satisfactorio de la instalación por la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital.

5. Si realizado el reconocimiento técnico se comprueba disconformidad entre lo instalado y lo autorizado, se notificarán al interesado las diferencias encontradas al objeto de que proceda a su subsanación en el plazo máximo de un mes.

6. Los titulares de derechos de uso del dominio público radioeléctrico estarán obligados a facilitar, en todo caso, la inspección de las instalaciones por los servicios técnicos de la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital, incluso de aquellas que hubieran sido objeto de certificación de instalación sustitutiva.

Por parte de los servicios de inspección de la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital se podrán dar instrucciones técnicas al titular de la estación al objeto de permitir la realización de la inspección de las instalaciones.

7. Para facilitar el reconocimiento técnico de las estaciones o las futuras inspecciones, el operador deberá tener un protocolo en materia de prevención de riesgos laborales que se aplicará cuando el personal inspector deba efectuar intervenciones en sus instalaciones.

Artículo 56. *Certificaciones de instalación sustitutivas del reconocimiento técnico previo a la autorización para la puesta en servicio.*

1. La certificación de instalación sustitutiva del reconocimiento técnico de la instalación por los servicios de inspección de la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital, previo a la autorización para la puesta en servicio, deberá ser firmada por un técnico competente en materia de telecomunicaciones y garantizará, al menos, los siguientes elementos:

a) Que el técnico competente ha revisado la estación que se pretende poner en servicio.
b) Que la instalación de la estación se ajusta al proyecto técnico aprobado.
c) Que cada certificación sustitutiva se refiere a una única estación.

2. Mediante resolución de la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital se establecerán los tipos de estaciones para las que se requiere una certificación de instalación sustitutiva del reconocimiento técnico previo a la autorización para la puesta en servicio.

3. No obstante lo señalado en los apartados anteriores, en la resolución de otorgamiento del título habilitante para el uso privativo del dominio público radioeléctrico, o en la aprobación de proyecto técnico y la correspondiente autorización para realizar la instalación si se realizara con posterioridad al otorgamiento del título, podrá exigirse el reconocimiento técnico de las instalaciones por la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital en los casos de instalaciones que, por su complejidad o características técnicas, requieran de dicho reconocimiento.

Artículo 57. *Certificado de niveles de exposición radioeléctrica.*

1. En el caso de certificación sustitutiva del acto de reconocimiento técnico, junto con la solicitud de autorización para la puesta en servicio de una estación o red de estaciones, se deberá incluir una certificación de niveles de exposición radioeléctrica, en el entorno urbano o donde haya permanencia habitual de personas, para cada estación fija con potencia isotrópica radiada equivalente superior a 10 vatios correspondiente a las redes y servicios a que se refiere el apartado 1 del artículo 53. La medición de niveles de exposición radioeléctrica deberá realizarse con una antelación no superior a tres meses a la fecha de presentación de la correspondiente certificación ante la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital.

2. A estos efectos, el certificado de niveles de exposición será realizado por un técnico competente en materia de telecomunicaciones.

El certificado de niveles considerará la exposición simultánea de los campos emitidos por todas las posibles estaciones radioeléctricas que influyan en cada uno de los puntos de medida, incluida la estación que se pretende poner en servicio, bien provengan de estaciones que presten servicios del mismo titular de derechos de uso del dominio público radioeléctrico o de titulares diferentes.

Para realizar este certificado, el técnico competente tomará medidas, al menos, en cinco puntos cercanos a la estación que se pretende poner en servicio, y que estará emitiendo de manera excepcional para poder realizar estas medidas. Mediante resolución del Secretario de Estado para la Sociedad de la Información y la Agenda Digital podrán establecerse los criterios para la elección de dichos puntos.

Las medidas se realizarán según el procedimiento previsto en la Orden CTE/23/2002, de 11 de enero, por la que se establecen condiciones para la presentación de determinados estudios y certificaciones por operadores de servicios de radiocomunicaciones.

El certificado de calibración de los equipos de medida se incorporará como anexo al citado certificado de niveles de exposición.

3. En el certificado de niveles de exposición se deberán incluir asimismo la evidencia de la existencia de la señalización de la estación radioeléctrica, basada en las normas técnicas sobre señales de seguridad, y del vallado instalado, cuando resulte exigible para restringir el acceso de personal no profesional en instalación, mantenimiento o inspección de estaciones radioeléctricas a zonas en las que pudieran superarse los límites establecidos en el anexo II del Reglamento que establece condiciones de protección del dominio público radioeléctrico, restricciones a las emisiones radioeléctricas y medidas de protección sanitaria frente a emisiones radioeléctricas, aprobado mediante el Real Decreto 1066/2001, de 28 de septiembre, según el proyecto técnico aprobado. En ese caso, el vallado deberá incorporar la señalización para prohibir el acceso al personal no profesional en instalación, mantenimiento o inspección de estaciones radioeléctricas, basada en las normas técnicas sobre señales de seguridad.

4. La Secretaría de Estado para la Sociedad de la Información y la Agenda Digital podrá exigir, en cualquier momento, la presentación del resultado de las medidas o cualquier otra documentación relacionada con el cumplimiento de las condiciones de la legislación vigente en materia de niveles de las emisiones radioeléctricas.

Artículo 58. *Solicitud de autorización para la puesta en servicio de las estaciones.*

1. De conformidad con lo señalado en el apartado 10 del artículo 49, la solicitud de autorización para la puesta en servicio deberá presentarse ante la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital en el plazo máximo de nueve meses desde la fecha de notificación de la aprobación del proyecto técnico y la correspondiente autorización para realizar la instalación, salvo que la resolución de aprobación del proyecto técnico hubiera fijado un plazo superior, o bien desde la fecha de presentación de la declaración responsable a que hace referencia el apartado 4 del artículo 51.

Transcurrido dicho plazo sin haberse presentado la solicitud, quedará sin efecto la aprobación del proyecto y la correspondiente autorización para realizar la instalación, o la mencionada presentación de la declaración responsable.

En el caso de que en dicho plazo se hubiese solicitado la autorización para la puesta en servicio mediante la presentación de la certificación sustitutiva del acto previo de reconocimiento de las instalaciones y, posteriormente, se hubiera dejado sin efecto la habilitación para la puesta en servicio, finalizado el mencionado plazo, quedará sin efecto la aprobación del proyecto y la correspondiente autorización para realizar la instalación.

La solicitud de autorización para la puesta en servicio se ajustará a los modelos que se establezcan por resolución del Secretario de Estado para la Sociedad de la Información y la Agenda Digital.

2. A la solicitud se acompañará la documentación siguiente:

a) Justificante del pago de las tasas de telecomunicaciones establecidas en el anexo I de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, correspondientes al acto de reconocimiento técnico de las instalaciones previo a la autorización para la puesta en servicio o, en su caso, a la presentación de la certificación de instalación sustitutiva del reconocimiento técnico de la instalación previo a la autorización para la puesta en servicio. El pago de dicha tasa está asociado a cada estación radioeléctrica que se pretenda poner en servicio.

b) Certificación de instalación de la estación radioeléctrica sustitutiva del reconocimiento técnico previo a la autorización para la puesta en servicio, cuando resulte exigible.

c) Certificación de niveles de exposición radioeléctrica, cuando resulte exigible.

Artículo 59. *Autorización para la puesta en servicio.*

1. La puesta en servicio se entenderá autorizada mediante la mera presentación de la solicitud correspondiente en los casos en que proceda la presentación de certificación de instalación sustitutiva del reconocimiento técnico previo a la autorización para la puesta en servicio.

En caso de que la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital constate que la documentación presentada no reúne los requisitos necesarios, dictará resolución motivada en un plazo máximo de tres meses, dejando sin efecto la habilitación para la puesta en servicio, y debiendo el titular proceder al cese inmediato de las emisiones.

2. En el resto de los casos, cuando se requiera efectuar un acto de inspección o de reconocimiento técnico de las instalaciones, la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital dictará resolución, en el plazo máximo de tres meses desde la solicitud de autorización para la puesta en servicio, autorizando o, en su caso, denegando la puesta en servicio y el inicio de la explotación de los derechos de uso privativo del dominio público radioeléctrico otorgado, y lo notificará al interesado.

3. En el caso de la autorización para la puesta en servicio de estaciones radioeléctricas para la prestación de servicios de radiodifusión sonora y de televisión por ondas terrestres, la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital informará a los órganos competentes del Estado y de las Comunidades Autónomas sobre las autorizaciones para la puesta en servicio de estaciones relacionadas con los títulos audiovisuales otorgados por ellos, en el plazo de quince días, contados desde la fecha de la resolución de autorización. Esta comunicación podrá ser sustituida por la publicación de esta información en la sede electrónica del Ministerio de Energía, Turismo y Agenda Digital.

Artículo 60. *Ausencia de perturbaciones y cumplimiento de disposiciones vigentes.*

La autorización para la puesta en servicio de cualquier estación quedará condicionada, en todo caso, a la ausencia de perturbaciones a otros servicios radioeléctricos autorizados, así como al cumplimiento de las disposiciones vigentes en materia de seguridad nacional, de servidumbres radioeléctricas o aeronáuticas, a lo indicado en el Reglamento que establece condiciones de protección del dominio público radioeléctrico, restricciones a las emisiones radioeléctricas y medidas de protección sanitaria frente a emisiones radioeléctricas, aprobado mediante el Real Decreto 1066/2001, de 28 de septiembre, o cualquier otra que le resulte de aplicación.

TÍTULO V

Servicios de radiocomunicaciones que utilizan el dominio público radioeléctrico para la defensa nacional

Artículo 61. *Uso del dominio público para la defensa nacional.*

1. Los servicios de radiocomunicaciones que utilizan el dominio público radioeléctrico para la defensa nacional y, en definitiva, las redes, sistemas, instalaciones y equipos de telecomunicaciones que desarrollen actividades esenciales para la defensa nacional, y que integren los medios destinados a ésta, tienen la consideración de servicio público.

2. El uso del dominio público radioeléctrico para la defensa nacional se realizará conforme a lo previsto en la Ley 9/2014, General de Telecomunicaciones, en el presente reglamento, y con carácter específico en el presente Título.

A tales efectos, los Ministerios de Defensa y de Energía, Turismo y Agenda Digital coordinarán la planificación del uso del espectro radioeléctrico por la Fuerzas Armadas en relación con las necesidades de la defensa nacional, a fin de asegurar, en la medida de lo posible, su compatibilidad con los servicios civiles.

Artículo 62. *Título habilitante para el uso del dominio público radioeléctrico destinado a las telecomunicaciones para la defensa nacional.*

1. El título habilitante para el uso del dominio público radioeléctrico destinado a las telecomunicaciones para la defensa nacional tendrá la consideración de uso privativo bajo la modalidad de autoprestación y adoptará la forma de afectación.

2. El Ministerio de Defensa deberá obtener de la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital, el título habilitante para la utilización del dominio público radioeléctrico, de acuerdo con lo establecido en este reglamento.

3. El procedimiento de obtención del título habilitante para el uso del dominio público radioeléctrico destinado a las telecomunicaciones para la defensa nacional seguirá, con carácter general, el procedimiento señalado en el presente reglamento para la obtención de título habilitante para uso privativo del dominio público radioeléctrico y para la instalación, así como para la puesta en servicio de las estaciones radioeléctricas correspondientes.

No obstante lo anterior, el Secretario de Estado para la Sociedad de la Información y la Agenda Digital, previo informe de la Comisión interministerial de los servicios de telecomunicaciones que utilizan el dominio público radioeléctrico para la defensa nacional, podrá establecer de manera excepcional modificaciones al procedimiento para la instalación y para la puesta en servicio de las estaciones radioeléctricas, por razones debidamente justificadas, cuando las estaciones radioeléctricas a instalar así lo requieran.

4. Para garantizar los intereses relacionados con la defensa nacional, la tramitación de los procedimientos de otorgamiento de títulos habilitantes para el uso del dominio público radioeléctrico destinado a las telecomunicaciones para la defensa nacional, que contengan información de carácter confidencial, quedará restringido a los funcionarios que designe la Comisión interministerial de los servicios de telecomunicaciones que utilizan el dominio público radioeléctrico para la defensa nacional.

Artículo 63. *Derecho a la protección frente a interferencias.*

1. Las estaciones radioeléctricas destinadas a la defensa nacional que cuenten con autorización para la puesta en servicio tienen derecho a la protección frente a interferencias perjudiciales, con el fin de asegurar una calidad técnicamente satisfactoria en su zona de servicio establecida en la correspondiente resolución de afectación o reserva de frecuencia, y podrán solicitar la intervención de los servicios técnicos de la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital.

2. La solicitud de intervención ante interferencias se ajustará al protocolo de actuación que se aprobará en la Comisión interministerial de los servicios de telecomunicaciones que utilizan el dominio público radioeléctrico para la defensa nacional.

Artículo 64. *Comisión interministerial de los servicios de telecomunicaciones que utilizan el dominio público radioeléctrico para la defensa nacional.*

1. Se crea la Comisión interministerial de los servicios de telecomunicaciones que utilizan el dominio público radioeléctrico para la defensa nacional, de conformidad con lo previsto en el artículo 4.3 de la Ley 9/2014, General de Telecomunicaciones, que se adscribe a la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital.

Su régimen jurídico y funcionamiento se ajustará a lo dispuesto para los órganos colegiados en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

2. La Comisión se ocupará del estudio e informe en las siguientes materias:

a) Coordinación de la planificación del uso del espectro radioeléctrico por la Fuerzas Armadas en relación con las necesidades de la defensa nacional, a fin de asegurar, en la medida de lo posible, su compatibilidad con los servicios civiles.

b) Elaboración de los programas de coordinación tecnológica precisos que faciliten la armonización, homologación y utilización, conjunta o indistinta, de los medios, sistemas y redes civiles y militares en el ámbito de las radiocomunicaciones.

c) Informar los procedimientos administrativos específicos necesarios para la instalación y para la puesta en servicio de determinadas estaciones radioeléctricas destinadas a la defensa nacional, designación de los funcionarios que tendrán acceso a la tramitación de los procedimientos correspondientes, y a la información recogida en el registro nacional de frecuencias. Igualmente, se determinará el protocolo para la transmisión de la información clasificada.

d) Fijación del protocolo de actuación en el caso de protección frente a interferencias perjudiciales.

3. La Comisión estará formada por el presidente, el vicepresidente y un máximo de diez vocales.

La Comisión estará presidida por el Subdirector General del órgano competente en la gestión del espectro radioeléctrico de la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital, que de acuerdo con lo establecido en el artículo 19.2.d) de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, dirimirá con su voto los empates.

El vicepresidente será el responsable del órgano competente en la gestión del espectro radioeléctrico, con rango de subdirección general, de la Secretaría de Estado de Defensa.

La Secretaría de Estado para la Sociedad de la Información y la Agenda Digital designará la mitad de los vocales que componen la Comisión y la Secretaría de Estado de Defensa designará la otra mitad de los vocales.

4. La Comisión se reunirá con periodicidad anual y cuando lo solicite alguna de las partes.

5. El funcionamiento de la Comisión será atendido con los medios personales, técnicos y presupuestarios disponibles en la Administración General del Estado.

TÍTULO VI

Mercado secundario del espectro

CAPÍTULO I

Disposiciones generales

Artículo 65. *Objeto y concepto.*

1. El objeto de este título es la regulación de los negocios jurídicos relativos al mercado secundario del espectro, cuyo fin es potenciar un uso más flexible y eficiente del dominio público radioeléctrico.

2. Los negocios jurídicos relativos al mercado secundario del espectro son los siguientes:

a) la transferencia de títulos habilitantes para el uso privativo del dominio público radioeléctrico,

b) la cesión de derechos de uso privativo del dominio público radioeléctrico,
c) la mutualización de los derechos de uso privativo del dominio público radioeléctrico,
d) la provisión de servicios mayoristas relevantes.

Artículo 66. *Autorización administrativa previa.*

Todo negocio jurídico relativo al mercado secundario del espectro, debe ser autorizado previamente por el Ministro de Energía, Turismo y Agenda Digital o por la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital, según corresponda.

El negocio jurídico de transferencia, de cesión, de mutualización o de provisión de servicios mayoristas relevantes efectuado que no hubiera obtenido dicha autorización administrativa previa será nulo de pleno derecho y se tendrá por no celebrado.

Artículo 67. *Exclusiones comunes.*

1. No son susceptibles de transferencia ni de cesión o mutualización, los siguientes derechos de uso del dominio público radioeléctrico

a) Los otorgados mediante autorizaciones generales e individuales de uso especial del dominio público radioeléctrico.

b) Los otorgados mediante afectación demanial.

c) Los relacionados con la defensa nacional, ni con el cumplimiento de las obligaciones de servicio público a que se refiere el Título III de la Ley General de Telecomunicaciones, impuestas en el título original.

d) Los obtenidos mediante concesiones con procedimiento de licitación hasta transcurridos dos años desde la fecha de otorgamiento del título original, para los casos de transferencia y cesión.

e) Los autorizados para fines experimentales y eventos de corta duración.

Artículo 68. *Requisitos.*

1. El titular del título habilitante para el uso del dominio público radioeléctrico a transferir, de los derechos de uso a ceder o los titulares de derechos de uso a mutualizar, o el titular de los derechos de uso sobre los que se pretende proporcionar servicios mayoristas relevantes, deberán encontrarse, a la fecha de autorización correspondiente al corriente del cumplimiento de cualquier obligación inherente al título habilitante para el uso del dominio público radioeléctrico del que es titular.

En el caso del abono de la tasa por reserva del dominio público radioeléctrico, se entenderá que se está al corriente del cumplimiento de esta obligación cuando, en el procedimiento de impugnación en vía administrativa o contencioso-administrativa interpuesto contra la liquidación de la tasa, se hubiese acordado la suspensión del acto impugnado, o bien cuando se hubiese autorizado el aplazamiento o fraccionamiento de su pago.

2. El nuevo titular o el cesionario de los derechos de uso, deberá reunir las condiciones que, de acuerdo con la Ley General de Telecomunicaciones y su normativa de desarrollo, resulten exigibles para la explotación de la red o la prestación del servicio al que se pretende destinar los derechos de uso. En el caso de transferencia, el nuevo titular deberá cumplir todos los requisitos exigidos en el presente reglamento para la obtención del título habilitante para el uso del dominio público radioeléctrico.

3. Las condiciones técnicas de uso de los títulos transferidos, y de los derechos cedidos o mutualizados, se ajustarán, en cualquier caso, a las establecidas en el Cuadro Nacional de Atribución de Frecuencias, en los planes técnicos correspondientes y en este reglamento, así como a las que, en su caso, estén fijadas en acuerdos internacionales, normativa de la Unión Europea y acuerdos de coordinación de frecuencias con otros países.

Asimismo, se deberán respetar las condiciones de uso del dominio público radioeléctrico que existieran en el título original, así como las condiciones aplicables recogidas en el presente reglamento, en particular las limitaciones derivadas de servidumbres radioeléctricas, limitaciones por razones de compatibilidad entre servicios, niveles máximos de emisión y protección de los centros de control de emisiones radioeléctricas de la Administración.

Artículo 69. *Normas comunes para la presentación y tramitación de solicitudes y documentación anexa.*

1. Los interesados en obtener autorización de los negocios jurídicos relativos al mercado secundario de espectro, deberán presentar sus solicitudes y la documentación adicional correspondiente ante la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital.

La solicitud deberá ir firmada conjuntamente por todos los intervinientes en el negocio jurídico de mercado secundario del espectro, con indicación del domicilio y de la información requerida para efectuar las notificaciones electrónicas.

2. La solicitud deberá ir acompañada de la siguiente documentación:

a) Documentos que acrediten la capacidad del solicitante, y en su caso, documentos que acrediten la representación, según lo señalado en los apartados 1 y 2 del artículo 31

b) En el caso de concesiones administrativas, certificación de que el nuevo titular de la transferencia o cesión, o el beneficiario del servicio mayorista relevante está inscrito en el Registro de Operadores previsto en el artículo 7 de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

c) En el caso de concesiones, declaración responsable de no estar incursos los solicitantes en ninguna de las prohibiciones de contratar reguladas en el texto refundido de la Ley de Contratos del Sector Público, aprobado mediante el Real Decreto Legislativo 3/2011, de 14 de noviembre.

d) Declaración de las personas extranjeras de someterse a la jurisdicción de los Juzgados y Tribunales españoles de cualquier orden para todas las incidencias que, de modo directo o indirecto, pudieran surgir de actos realizados al amparo del título habilitante concedido para el uso del dominio público radioeléctrico, con renuncia, en su caso, al fuero jurisdiccional extranjero que pudiera corresponder al solicitante.

e) Referencia del título o títulos habilitantes para el uso del dominio público radioeléctrico afectados por el negocio jurídico.

f) Copia del negocio jurídico a suscribir entre los titulares.

g) Características de las redes y servicios en los que se prevé utilizar los derechos de uso del dominio público objeto del negocio jurídico.

3. Si la documentación aportada no reuniera los requisitos exigidos, se requerirá al interesado para que, en el plazo de 10 días hábiles, desde el siguiente al de recepción del requerimiento, subsane la falta o acompañe los documentos preceptivos, con advertencia de que, si no lo hiciese, se le tendrá por desistido de su solicitud, previa resolución de la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital, de acuerdo con lo establecido en el artículo 68 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

4. La Secretaría de Estado para la Sociedad de la Información y la Agenda Digital, antes de dictar resolución podrá requerir al solicitante cuanta información o aclaraciones considere convenientes sobre su solicitud o sobre los documentos presentados.

5. La Secretaría de Estado para la Sociedad de la Información y la Agenda Digital dictará resolución autorizando o denegando motivadamente el negocio jurídico relativo al mercado secundario del espectro, sin perjuicio de la aplicación de la normativa de defensa de la competencia. Dicha resolución pondrá fin a la vía administrativa.

6. El plazo para dictar resolución será de tres meses desde la entrada de la solicitud en cualquiera de los registros de la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital. Transcurrido el plazo sin haberse notificado resolución expresa, deberán entenderse desestimadas las solicitudes, sin perjuicio de la obligación de la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital de resolver expresamente, de acuerdo con lo dispuesto en el artículo 24 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Artículo 70. *Denegación de solicitudes.*

La Secretaría de Estado para la Sociedad de la Información y la Agenda Digital denegará las solicitudes de autorización de negocios jurídicos relativos al mercado secundario de espectro por alguna de las siguientes causas:

a) Cuando concurra alguna de las exclusiones comunes señaladas en el artículo 67, o no se haya acreditado por los solicitantes los requisitos señalados en el artículo 68.

b) Cuando se derive una situación de acaparamiento de derechos de uso de dominio público radioeléctrico, y en particular cuando implique la superación de los límites a la cantidad de derechos de uso del dominio público radioeléctrico por un mismo titular que se hubiesen establecido conforme a lo previsto en este reglamento, sin perjuicio de lo establecido en el apartado 4 del artículo 88.

c) Cuando exista riesgo de una restricción de la competencia en el mercado. En este caso, se solicitará previamente informe a la Comisión Nacional de los Mercados y la Competencia.

d) Cuando el titular de los derechos de uso correspondientes, se encuentre incurso en un procedimiento administrativo del que pueda derivarse la revocación del título habilitante para el uso del dominio público radioeléctrico.

CAPÍTULO II

Transferencia de títulos que habilitan al uso privativo del dominio público radioeléctrico

Artículo 71. *Concepto y ámbito subjetivo.*

1. En la transferencia de títulos habilitantes para el uso privativo del dominio público radioeléctrico se transmite la titularidad del título habilitante y, en consecuencia, se transmite la totalidad de los derechos de uso privativo del dominio público radioeléctrico derivados del título, por todo el periodo de tiempo que reste de vigencia y en todo el ámbito geográfico del título.

2. La transferencia podrá autorizarse para cualquier título habilitante para el uso del dominio público radioeléctrico sin más limitaciones que las establecidas en este reglamento.

3. No podrá realizarse la transferencia parcial de títulos habilitantes para el uso del dominio público radioeléctrico, bien sea en cuanto a los derechos de uso privativo del dominio público radioeléctrico derivados del título, o en lo que se refiere al ámbito geográfico del título.

4. A los efectos de este reglamento, se entenderá que existe transferencia de título habilitante para el uso privativo del dominio público radioeléctrico en los siguientes supuestos:

a) Cuando se transmita el cien por cien de las acciones o participaciones de la entidad que sea titular del título habilitante o de un porcentaje menor que suponga alteración de su control efectivo.

b) En los casos de fusión de empresas en los que participe el titular del título habilitante, para que la entidad absorbente o resultante de la fusión quede subrogada en todos los derechos y obligaciones derivados del título.

c) En los supuestos de escisión, aportación o transmisión de empresas que sean titulares del título habilitante, para que la entidad resultante o beneficiaria quede subrogada en todos los derechos y obligaciones derivados del título.

Artículo 72. *Subrogación de derechos y obligaciones.*

1. El nuevo titular se subrogará en todos los derechos y obligaciones del anterior titular, derivados del título a transferir. En particular, en el caso de las concesiones otorgadas por el procedimiento de licitación, el nuevo titular se subrogará en todas las condiciones especificadas en el pliego de bases por el que se rigió dicho procedimiento, así como en todos los compromisos asumidos por el titular en la oferta que sirvió de base para la adjudicación.

2. Los proyectos técnicos aprobados y las autorizaciones para la puesta en servicio, correspondientes a estaciones asociadas al título habilitante para el uso del dominio público radioeléctrico objeto de transferencia, mantendrán su validez para el nuevo titular. A estos efectos, en el plazo de un mes a partir de la fecha de autorización de la transferencia, el nuevo titular deberá remitir a la Secretaría de Estado para la Sociedad de la Información y la

Agenda Digital la relación de estaciones que va a continuar utilizando. Transcurrido dicho plazo, la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital cancelará de oficio el resto de las estaciones.

Artículo 73. *Autorización de la transferencia.*

1. La autorización de la transferencia de títulos habilitantes para el uso del dominio público radioeléctrico se realizará de acuerdo con el procedimiento general señalado en el Capítulo I de este título.

2. En este caso se acompañará además a la solicitud la documentación siguiente:

a) Declaración responsable del anterior titular de haber comunicado al nuevo titular las condiciones asociadas al título habilitante para el uso del dominio público radioeléctrico objeto del negocio jurídico, incluyendo los aspectos técnicos, tales como características de emisión, compatibilidad entre servicios o resolución de interferencias.

b) Declaración responsable del nuevo titular de que conoce y asume la responsabilidad en el uso del dominio público radioeléctrico objeto del negocio jurídico de acuerdo con las condiciones exigibles asociadas al título habilitante para el uso del dominio público radioeléctrico correspondiente, incluyendo los aspectos técnicos, tales como características de emisión, compatibilidad entre servicios o resolución de interferencias.

3. Cuando se trate de una concesión, en el caso de que se autorice la transferencia, se procederá a la inscripción del nuevo titular en el Registro Público de Concesiones.

4. La autorización de la transferencia podrá ser denegada por las causas señaladas en el artículo 70.

Artículo 74. *Transferencias sucesivas.*

Los títulos habilitantes para el uso privativo del dominio público radioeléctrico que hayan sido transferidos podrán ser objeto de nuevas transferencias.

No obstante lo anterior, si los títulos habilitantes para el uso del dominio público radioeléctrico se otorgaron mediante un procedimiento de licitación y en el pliego de bases regulador del mismo se hubiera fijado un período mínimo en el que dichos títulos habilitantes no podrían ser objeto de transferencia, las transferencias sucesivas no podrán efectuarse hasta que transcurra dicho período desde la fecha en que la anterior transferencia hubiera sido autorizada.

CAPÍTULO III

Cesión de derechos de uso privativo del dominio público radioeléctrico

Artículo 75. *Concepto y ámbito subjetivo.*

1. En la cesión de derechos de uso privativo del dominio público radioeléctrico se transmite el derecho a utilizar determinadas frecuencias o bandas de frecuencias vinculadas al título.

2. Son susceptibles de cesión los derechos de uso privativo del dominio público radioeléctrico atribuidos a los servicios con frecuencias reservadas en las bandas a las que hace referencia el anexo 1 de este reglamento.

3. La cesión podrá comprender todas o parte de las frecuencias cuyos derechos de uso han sido otorgados, en toda o parte del área geográfica sobre la que el título habilitante para el uso del dominio público radioeléctrico original otorgó los derechos de uso del dominio público radioeléctrico y por todo o una parte del periodo de tiempo que reste de vigencia de dicho título.

Una cesión de todas las frecuencias, en toda el área geográfica y por todo el periodo de tiempo que reste de vigencia del título correspondiente, será considerada una transferencia del título habilitante para el uso del dominio público radioeléctrico, y su autorización deberá tramitarse como conforme a lo señalado en el capítulo anterior.

Artículo 76. *Autorización de la cesión.*

1. La autorización de la cesión de títulos habilitantes para el uso del dominio público radioeléctrico se realizará de acuerdo con el procedimiento general señalado en el Capítulo I de este título.

2. En este caso se acompañará además a la solicitud y documentación anexa señalada en el artículo 69.2, la siguiente documentación:

a) Declaración responsable del cedente de haber comunicado al cesionario condiciones asociadas al título habilitante para el uso del dominio público radioeléctrico objeto del negocio jurídico, incluyendo los aspectos técnicos, tales como características de emisión, compatibilidad entre servicios o resolución de interferencias.

b) Declaración responsable del cesionario de que conoce y asume la responsabilidad en el uso del dominio público radioeléctrico objeto del negocio jurídico de acuerdo con las condiciones exigibles asociadas al título habilitante para el uso del dominio público radioeléctrico correspondiente, incluyendo los aspectos técnicos, tales como características de emisión, compatibilidad entre servicios o resolución de interferencias.

c) Identificación del dominio público radioeléctrico objeto del negocio jurídico y zona geográfica de utilización, y determinación del periodo temporal de la cesión.

3. Cuando se trate de una concesión, en el caso de que se autorice la cesión, se procederá a su anotación en el Registro Público de Concesiones.

4. Los intervinientes deberán comunicar a la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital la extinción o cualquier modificación del negocio jurídico de cesión, que pueda producirse con anterioridad a que expire el período de tiempo de vigencia por el que fue suscrito.

5. La autorización de la cesión podrá ser denegada por las causas señaladas en el artículo 70, y cuando la cesión de los derechos de uso del dominio público radioeléctrico contemplados pudieran comprometer el cumplimiento por el cedente de las obligaciones asumidas frente a la Administración en relación con el título habilitante para el uso del dominio público radioeléctrico objeto del negocio jurídico.

A los efectos de los posibles límites a la cantidad de derechos de uso del dominio público radioeléctrico por un mismo titular, se entenderá que el cedente no ostenta los derechos de uso del dominio público radioeléctrico objeto de cesión en la zona geográfica correspondiente y durante el periodo de tiempo en que la cesión se mantenga vigente.

Artículo 77. *Derechos y obligaciones específicos en la cesión.*

1. El cedente será responsable ante la Administración del cumplimiento de las obligaciones asociadas al título habilitante para el uso del dominio público radioeléctrico original, salvo aquellas que correspondan al cesionario especificadas en este reglamento. En particular, el cedente será responsable del abono de la tasa por reserva de dominio público radioeléctrico correspondiente a dicho título habilitante, incluyendo la tasa correspondiente a los derechos de uso que hubieran sido objeto de cesión.

2. El cesionario será responsable del uso del dominio público radioeléctrico objeto de cesión, de acuerdo con las condiciones técnicas exigibles; en particular, será responsable de la utilización de las estaciones de acuerdo con las condiciones técnicas autorizadas, de la compatibilidad con otros servicios, así como de posibles interferencias perjudiciales que pudieran causar y de su resolución. Asimismo, el cesionario deberá presentar los proyectos técnicos de las estaciones y las correspondientes solicitudes de autorización para realizar la instalación, las solicitudes de autorización para la puesta en servicio y las certificaciones anuales de niveles de exposición radioeléctrica, en lo que se refiere a los derechos de uso objeto de cesión.

3. Los proyectos técnicos aprobados y las autorizaciones para la puesta en servicio, correspondientes a las estaciones del cedente asociadas a las frecuencias y al ámbito geográfico objeto de la cesión, mantendrán su validez para el cesionario. A estos efectos, en el plazo de un mes a partir de la fecha de autorización de la cesión, el cedente y el cesionario deberán remitir a la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital un escrito firmado conjuntamente en el que se relacionen dichas estaciones.

Transcurrido dicho plazo, la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital cancelará de oficio el resto de las estaciones.

Artículo 78. *Cesiones sucesivas.*

Los derechos de uso privativo del dominio público radioeléctrico que hayan sido cedidos no podrán ser objeto de nuevas cesiones por el cesionario.

Artículo 79. *Revocación de la autorización de la cesión.*

La Secretaría de Estado para la Sociedad de la Información y la Agenda Digital podrá acordar, mediante resolución motivada, la revocación de la autorización de la cesión de derechos de uso del dominio público radioeléctrico y, en consecuencia, la extinción del negocio jurídico autorizado, por las siguientes causas:

g) El incumplimiento de las condiciones esenciales de la cesión en los términos en que fue autorizada.

h) La existencia de interferencias perjudiciales o incompatibilidades electromagnéticas que degraden la calidad de los servicios prestados u otros previamente autorizados, originados como consecuencia de la cesión.

i) La revocación o extinción del título habilitante para el uso del dominio público radioeléctrico original.

CAPÍTULO IV

Mutualización de los derechos de uso del dominio público radioeléctrico

Artículo 80. *Concepto y ámbito objetivo.*

1. En la mutualización o puesta en común de derechos, dos o más titulares de derechos de uso del dominio público radioeléctrico, o uno o más titulares de derechos de uso con uno o más operadores que no disponen de derechos de uso objeto de la mutualización, comparten en una determinada zona geográfica los derechos individuales de uso. Las frecuencias mutualizadas pasan a ser de utilización conjunta de los participantes en el acuerdo de mutualización, manteniendo los mutualistas la titularidad jurídica de sus derechos de uso objeto de la mutualización.

2. La mutualización de frecuencias puede conllevar tanto la compartición de elementos de la red como el uso de la infraestructura desplegada por cada uno de los mutualistas a través de los oportunos mecanismos de coordinación técnica.

La gestión técnica de las frecuencias objeto de mutualización puede ser realizada por uno o varios de los operadores que mutualizan sus frecuencias, o bien ser encomendada a un tercer agente, diferente a los operadores que participan en la mutualización, sin que este tercer agente ostente los derechos de uso de las frecuencias para la prestación de servicios.

3. Son susceptibles de mutualización, o puesta en común, los derechos de uso privativo del dominio público radioeléctrico correspondientes a las bandas de frecuencias habilitadas para la prestación de servicios de comunicaciones electrónicas.

4. La mutualización de derechos de uso no exime a cada titular, con los derechos de uso de los que es titular, del cumplimiento de las obligaciones individuales que tenga asumidas, en su caso, frente a la Administración.

5. La mutualización podrá ser de todas o parte de las frecuencias cuyos derechos de uso han sido otorgados, en toda o parte del área geográfica sobre la que el título habilitante para el uso del dominio público radioeléctrico original otorgó los derechos de uso del dominio público radioeléctrico y por todo o una parte del tiempo que reste de vigencia de los títulos.

6. Los derechos que hayan sido objeto de mutualización no pueden ser cedidos ni ser objeto simultáneamente de otras mutualizaciones. Podrán prestarse servicios mayoristas haciendo uso de los derechos mutualizados, en las condiciones previstas en el presente título, previo acuerdo de todos los mutualistas. Serán susceptibles de transferencia, en las condiciones previstas en este título, los derechos individuales de uso que hubieran sido objeto de mutualización.

Artículo 81. *Autorización de la mutualización de derechos de uso.*

1. La autorización de la mutualización de derechos de uso del dominio público radioeléctrico se realizará de acuerdo con el procedimiento general señalado en el Capítulo I de este título.

2. En este caso se acompañará además a la solicitud y documentación anexa señalada en el artículo 69.2, la siguiente documentación:

a) Declaración responsable de los mutualistas de que conocen y asumen la responsabilidad en el uso del dominio público radioeléctrico objeto del negocio jurídico de acuerdo con las condiciones exigibles asociadas a los títulos habilitantes para el uso del dominio público radioeléctrico correspondientes, incluyendo los aspectos técnicos, tales como características de emisión, compatibilidad entre servicios o resolución de interferencias.

b) Identificación del dominio público radioeléctrico objeto del negocio jurídico y zona geográfica de utilización, y determinación del periodo temporal de la mutualización.

3. Cuando se trate de una concesión, en el caso de que se autorice la mutualización, se procederá a su anotación en el Registro Público de Concesiones.

4. Los intervinientes deberán comunicar a la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital la extinción o cualquier modificación del negocio jurídico de mutualización, que pueda producirse con anterioridad a que expire el período de tiempo de vigencia por el que fue suscrito.

5. La autorización de la mutualización podrá ser denegada por las causas señaladas en el artículo 70, y cuando la mutualización de los derechos de uso del dominio público radioeléctrico contemplados pudieran comprometer el cumplimiento por alguno de los participantes de las obligaciones asumidas frente a la Administración en relación con el título habilitante para el uso del dominio público radioeléctrico objeto del negocio jurídico.

A los efectos de los posibles límites a la cantidad de derechos de uso del dominio público radioeléctrico por un mismo titular, se entenderá que cada uno de los mutualistas ostentan la totalidad de los derechos de uso del dominio público radioeléctrico objeto de mutualización en la zona geográfica correspondiente y durante el periodo de tiempo en que la mutualización se mantenga vigente.

6. El titular de cada uno de los derechos objeto de mutualización se mantendrá como único responsable ante la Administración a efectos de posibles modificaciones del título habilitante para el uso del dominio público radioeléctrico original o de cualquier otro trámite relacionado con el mismo, incluyendo la obligación del abono de la tasa por reserva de dominio público radioeléctrico, la presentación de proyectos técnicos, la solicitud de autorización para la puesta en servicio, o la presentación de las certificaciones anuales de niveles de exposición radioeléctrica.

7. Una vez que concluya la vigencia del negocio jurídico, cada uno de los titulares originales recuperarán la exclusividad de los derechos de uso mutualizados.

Artículo 82. *Revocación de la autorización de la mutualización de derechos de uso.*

La Secretaría de Estado para la Sociedad de la Información y la Agenda Digital podrá acordar, mediante resolución motivada, la revocación de la autorización de la mutualización de derechos de uso del dominio público radioeléctrico y, en consecuencia, la extinción del negocio jurídico autorizado, por las siguientes causas:

a) El incumplimiento de las condiciones esenciales establecidas en la resolución de autorización del negocio jurídico.

b) La existencia de interferencias perjudiciales o incompatibilidades electromagnéticas que degraden la calidad de los servicios prestados u otros previamente autorizados, originados como consecuencia de la mutualización.

c) La revocación o extinción de cualquiera de los títulos habilitantes para el uso del dominio público radioeléctrico afectados por la mutualización

CAPÍTULO V

Provisión de servicios mayoristas relevantes

Artículo 83. *Concepto y ámbito objetivo.*

1. Un servicio mayorista relevante consiste en cualquier acuerdo entre dos operadores de comunicaciones electrónicas que sean titulares de derechos de uso del dominio público radioeléctrico en bandas de frecuencia con limitación de número otorgadas mediante procedimiento de licitación para prestación de servicios a terceros, en virtud del cual uno de los operadores, que actúa como prestador del servicio, permite a los clientes del otro operador, que actúa como prestatario del servicio, recibir servicios en cuya prestación se hace uso del espectro y los elementos de la red del primero.

En virtud de un servicio mayorista relevante el operador prestador del servicio comparte el derecho de uso del dominio público radioeléctrico del que es titular entre sus propios clientes y los clientes del operador prestatario del servicio.

Un caso particular de servicio mayorista relevante lo constituyen los acuerdos de itinerancia entre operadores.

2. Un servicio mayorista relevante no supone transferencia de títulos habilitantes para el uso del dominio público radioeléctrico de los operadores intervinientes manteniendo cada uno de ellos la titularidad de los mismos, de manera que el operador que presta el servicio sigue siendo el encargado de la gestión real y efectiva de las frecuencias utilizadas

3. La prestación de un servicio mayorista relevante podrá comprender todas o parte de las frecuencias cuyos derechos de uso corresponden al prestador, en toda o parte del área geográfica a que habilita el uso del título habilitante para el uso del dominio público radioeléctrico del prestador y por todo o una parte del tiempo que reste de vigencia del título del prestador.

Artículo 84. *Autorización de negocios jurídicos para la provisión de servicios mayoristas relevantes.*

1. La autorización de los negocios jurídicos para la provisión servicios mayoristas relevantes se realizará de acuerdo con el procedimiento general señalado en el Capítulo I de este título.

2. En este caso se acompañará además a la solicitud y documentación anexa señalada en el artículo 69.2, la identificación del dominio público radioeléctrico objeto del negocio jurídico y zona geográfica de utilización, y determinación del periodo temporal en que se prestará el servicio.

3. En el caso de que se autorice el servicio mayorista relevante, se procederá a su anotación en el Registro Público de Concesiones.

4. Los intervinientes deberán comunicar a la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital la extinción o cualquier modificación del negocio jurídico para la provisión del servicio mayorista relevante, que pueda producirse con anterioridad a que expire el período de tiempo de vigencia por el que fue suscrito.

5. La autorización de los negocios jurídicos para la provisión de servicios mayoristas relevantes podrá ser denegada por las causas señaladas en el artículo 70, y por las siguientes:

a) Cuando los derechos de uso del dominio público radioeléctrico correspondiente pudieran comprometer el cumplimiento por parte del prestador del servicio de las obligaciones correspondientes al título habilitante para el uso del dominio público radioeléctrico y, en particular, aquellas asumidas frente a la Administración en relación con dicho título habilitante objeto del negocio jurídico.

b) En el caso de que no se respeten las condiciones o limitaciones que se hubieran establecido para la prestación de estos servicios mayoristas en los correspondientes pliegos de bases del procedimiento de licitación para el otorgamiento de los títulos.

c) Cuando el prestador y el prestatario del servicio mayorista relevante sean titulares de derechos de uso del dominio público radioeléctrico y no se garantice un uso eficaz y eficiente del espectro radioeléctrico. A estos efectos, se tomará en consideración el plazo de tiempo transcurrido desde el otorgamiento de los títulos habilitantes para el uso del dominio público

radioeléctrico, las áreas geográficas en las que se pretende prestar el servicio, así como la innovación tecnológica en las bandas de frecuencias correspondientes.

A los efectos de los posibles límites a la cantidad de derechos de uso del dominio público radioeléctrico por un mismo titular, se entenderá que el prestador del servicio mayorista relevante ostenta la totalidad de los derechos de uso del dominio público radioeléctrico utilizado en la provisión del servicio, en la zona geográfica correspondiente y durante el periodo de tiempo en que el servicio se mantenga vigente.

Artículo 85. *Revocación de la autorización de negocios jurídicos para la provisión de servicios mayoristas relevantes.*

La Secretaría de Estado para la Sociedad de la Información y la Agenda Digital podrá acordar, mediante resolución motivada, la revocación de la autorización del negocio jurídico para la provisión de servicios mayoristas relevantes y, en consecuencia, la extinción del negocio jurídico autorizado, por las siguientes causas:

a) El incumplimiento de las condiciones esenciales establecidas en la resolución de autorización del negocio jurídico.

b) La existencia de interferencias perjudiciales o incompatibilidades electromagnéticas que degraden la calidad de los servicios prestados u otros previamente autorizados, originados como consecuencia de la provisión del servicio mayorista relevante.

c) La revocación o extinción del título habilitante para el uso del dominio público radioeléctrico del prestador del servicio mayorista relevante.

CAPÍTULO VI

Acaparamiento de recursos de dominio público radioeléctrico

Artículo 86. *Medidas contra comportamientos especulativos o acaparamiento de derechos de uso del dominio público radioeléctrico.*

1. En el Cuadro Nacional de Atribución de Frecuencias o en los pliegos reguladores de los procedimientos de licitación para el otorgamiento de títulos habilitantes para el uso del dominio público radioeléctrico se podrán establecer cautelas para evitar comportamientos especulativos o acaparamiento de derechos de uso del dominio público radioeléctrico.

En particular, estas cautelas podrán consistir, entre otras, en:

a) la fijación de límites en la cantidad de frecuencias a utilizar por un mismo operador o grupo empresarial.

b) la fijación de plazos estrictos para la explotación de los derechos de uso por parte de su titular.

2. Estas cautelas se establecerán y aplicarán de manera que sean proporcionadas, no discriminatorias y transparentes.

Artículo 87. *Venta o cesión de derechos de uso de radiofrecuencias.*

1. Para asegurar el cumplimiento de las cautelas establecidas en el artículo anterior, el Ministerio de Energía, Turismo y Agenda Digital, de manera motivada, proporcionada, no discriminatoria y transparente podrá ordenar la venta o la cesión de derechos de uso de radiofrecuencias.

2. En el caso de que no se hubiese procedido a la venta o la cesión de derechos de uso de radiofrecuencias en el plazo que se hubiera fijado para ello, se procederá conforme a lo previsto en el apartado 8 del artículo 88.

Artículo 88. *Superación de los límites en la cantidad de frecuencias a utilizar por un mismo operador.*

1. Los titulares de derechos de uso del dominio público radioeléctrico deberán cumplir los límites en la cantidad de frecuencias a utilizar por un mismo operador o grupo empresarial que puedan haberse establecido normativamente, en el Cuadro Nacional de Atribución de

Frecuencias o en los pliegos reguladores de los procedimientos de licitación para el otorgamiento de títulos habilitantes para el uso del dominio público radioeléctrico.

2. El cómputo de la disponibilidad de las frecuencias incluirá tanto si dicha disponibilidad viene derivada de la titularidad de concesiones demaniales, de negocios jurídicos relativos al mercado secundario del espectro, o de operaciones societarias o de concentración empresarial que impliquen la disponibilidad en el uso de las frecuencias.

3. Los límites se aplicarán al operador directamente o al grupo de empresas del que forme parte en los términos establecidos por el artículo 42 del Código de Comercio.

4. El Ministro de Energía, Turismo y Agenda Digital podrá permitir, tanto en los pliegos del procedimiento de licitación de títulos habilitantes para el uso del dominio público radioeléctrico como en las autorizaciones previas para celebrar negocios jurídicos relativos al mercado secundario del espectro, superar los límites establecidos en la cantidad de frecuencias a utilizar por un mismo operador o grupo empresarial siempre y cuando se asuman por los licitadores o titulares de derechos de uso del dominio público radioeléctrico compromisos previstos en los pliegos que, en su conjunto, favorezcan y fomenten la competencia.

Estos compromisos, sobre los que la Comisión Nacional de los Mercados y la Competencia emitirá informe en relación con el fomento de la competencia, consisten en la provisión de servicios mayoristas, fijación de condiciones técnicas y económicas de acceso a sus redes y servicios o contratación de determinados servicios.

El Ministerio de Energía, Turismo y Agenda Digital realizará un seguimiento del cumplimiento de dichos compromisos y, en el caso de que acredite que los mismos no se están cumpliendo, adoptará las medidas oportunas para garantizar que vuelvan a cumplirse los límites establecidos en la cantidad de frecuencias a utilizar por un mismo operador o grupo empresarial conforme a lo señalado en los apartados siguientes, sin perjuicio de otras actuaciones que pueda realizar de acuerdo con lo establecido en el presente reglamento.

5. En los procedimientos de licitación de títulos habilitantes para el uso del dominio público radioeléctrico, salvo que se aplique la posibilidad prevista en el apartado anterior, se tendrá en cuenta el cumplimiento de los límites en la disponibilidad de frecuencias por un mismo operador, de forma que si la adjudicación de la concesión demanial solicitada o por la que puja un licitador implicara que dicho licitador superara los límites establecidos, se excluirá del concurso la oferta o no será validada en la subasta la puja que produjera dicho efecto.

6. En el caso de que se superaran los límites en la disponibilidad de frecuencias por un mismo operador o grupo empresarial, y no se aplique la posibilidad prevista en el apartado 4, la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital adoptará las medidas oportunas para garantizar que vuelvan a cumplirse los límites citados, sin perjuicio de las responsabilidades que puedan derivarse para ese operador o grupo empresarial.

A tal efecto la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital otorgará al operador o grupo empresarial un plazo de cinco meses a contar desde que se produjo la situación que determinó la superación de los límites o de dos meses desde que la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital tuvo conocimiento de dicha situación para que proceda a la transferencia de los títulos habilitantes para el uso del dominio público radioeléctrico oportunos o la cesión de derechos de uso, que posibilite el cumplimiento de los límites. Mediante resolución de la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital se podrán fijar unos plazos diferentes en función de la cantidad de espectro afectada, de las bandas de frecuencias afectadas, de los servicios que se vienen prestando a través de esas bandas de frecuencia o de la situación competitiva del mercado y la existencia de posibles adquirentes.

7. Las transferencias de títulos habilitantes o cesión de derechos de uso del dominio público radioeléctrico que se materialicen como consecuencia de lo indicado en el párrafo anterior deben cumplir lo establecido en el presente Título y en particular deben ser autorizadas previamente por la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital.

8. Si no se materializan las mencionadas transferencias o cesiones de derechos de uso, la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital requerirá al

operador o grupo empresarial para que en el plazo de quince días identifique los títulos habilitantes para el uso del dominio público radioeléctrico que revertirán al Estado.

La identificación de estos títulos habilitantes debe referirse a títulos íntegros, no siendo posible fraccionar los títulos por bloques de frecuencias ni por ámbitos territoriales.

9. Una vez identificados los títulos, el órgano competente del Ministerio de Energía, Turismo y Agenda Digital procederá a formalizar su extinción.

TÍTULO VII

Duración, modificación, extinción y revocación de los títulos habilitantes para el uso del dominio público radioeléctrico

Artículo 89. *Duración de los títulos habilitantes para el uso del dominio público radioeléctrico.*

1. Los títulos habilitantes para el uso especial del dominio público radioeléctrico en el caso de autorizaciones generales se otorgarán por un período de tiempo inicial que finalizará el 31 de diciembre del año natural en que cumpla su quinto año de vigencia, renovable por períodos sucesivos de cinco años en función de las disponibilidades y previsiones de la planificación de dicho recurso, salvo que mediante una orden se indiquen otras condiciones.

2. Los títulos habilitantes para el uso especial del dominio público radioeléctrico en el caso de autorizaciones individuales conservarán su vigencia mientras su titular no manifieste su renuncia o sea revocada por alguno de los supuestos previstos en su normativa, salvo que mediante una orden se indiquen otras condiciones.

3. Los títulos habilitantes para el uso privativo del dominio público radioeléctrico sin limitación de número de titulares se otorgarán, con carácter general, por un período de tiempo inicial que finalizará el 31 de diciembre del año natural en que cumpla su quinto año de vigencia, renovable de manera automática por períodos sucesivos de cinco años en función de las disponibilidades y previsiones de la planificación de dicho recurso.

6. Los títulos habilitantes para el uso privativo del dominio público radioeléctrico con limitación de número de titulares obtenidos mediante un procedimiento de licitación tendrán la duración prevista en los correspondientes procedimientos de licitación que, en todo caso, será como máximo de veinte años, incluyendo posibles prórrogas y sin posibilidad de renovación automática.

A la hora de determinar en el procedimiento de licitación la duración concreta de los derechos de uso, se tendrán en cuenta, entre otros criterios:

a) Las inversiones que se exijan y los plazos para su amortización.

b) Las obligaciones vinculadas a los derechos de uso, como la cobertura mínima que se imponga.

c) Las bandas de frecuencias cuyos derechos de uso se otorguen.

4. Los títulos habilitantes para el uso privativo del dominio público radioeléctrico reservado para servicios de radiodifusión sonora y de televisión digital terrestre tendrán la misma vigencia que el título para la prestación del servicio de comunicación audiovisual correspondiente y serán renovados cuando se produzca la renovación del título audiovisual correspondiente.

No obstante lo anterior, dichos títulos habilitantes para el uso privativo del dominio público radioeléctrico podrán ser objeto de extinción o revocación cuando se produzca alguna de las condiciones indicadas en este reglamento. En este caso, la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital comunicará dicha extinción o revocación a las autoridades competentes para el otorgamiento del título para la prestación del servicio de comunicación audiovisual correspondiente.

5. Los títulos habilitantes para el uso privativo del dominio público radioeléctrico correspondientes a recursos orbita-espectro tendrán la duración que se señale en el otorgamiento de dicho título habilitante y, en todo caso, por un período de tiempo máximo de veinte años. Su renovación se producirá en las condiciones que se señalen en el título habilitante para el uso del dominio público radioeléctrico y estará condicionada en todo caso

a que se mantenga por la UIT la reserva del recurso orbita-espectro a favor del Reino de España.

6. Los títulos habilitantes para el uso privativo del dominio público radioeléctrico correspondientes a fines experimentales y eventos de corta duración, tendrán la duración que se señale en el otorgamiento de dicho título habilitante, que no podrá ser superior a seis meses en las emisiones con fines experimentales y de un mes en el caso de eventos de corta duración.

Artículo 90. *Modificación de los títulos habilitantes para el uso del dominio público radioeléctrico.*

1. Se entenderá por modificación del título habilitante para el uso del dominio público radioeléctrico la alteración del ámbito geográfico, del periodo de vigencia de los derechos otorgados, de las frecuencias, de las potencias, de la banda de frecuencias, o cualquier otra característica técnica del título habilitante original, siempre que de la misma no se derive una imposibilidad de atender el fin para el que se hubiera otorgado el derecho de uso del dominio público radioeléctrico.

2. El Ministerio de Energía, Turismo y Agenda Digital, con arreglo a los principios de objetividad y proporcionalidad, podrá modificar, previa audiencia del interesado, el título habilitante para el uso del dominio público radioeléctrico, en cualquier momento durante el período de su vigencia, cuando concurra alguna de las circunstancias siguientes:

a) Adecuación al Cuadro Nacional de Atribución de Frecuencias o a la normativa comunitaria en materia de armonización del uso de las bandas de frecuencias.

b) Por razones de uso eficaz y eficiente del dominio público radioeléctrico de acuerdo con lo previsto en este reglamento.

c) Cumplimiento de obligaciones derivadas de acuerdos internacionales, o relacionados con la coordinación internacional de frecuencias.

d) Obsolescencia de la tecnología utilizada, cuando existan alternativas que, sin pérdida de los objetivos del servicio a prestar, redunden en una explotación más eficiente del espectro radioeléctrico.

e) Circunstancias sobrevenidas durante el periodo de vigencia del título habilitante para el uso del dominio público radioeléctrico, tales como nuevas servidumbres radioeléctricas, compatibilidad con nuevos servicios de radiocomunicaciones, límites que se hubieran establecido en relación con la cantidad de espectro que podrá ser reservado en favor de un mismo titular, o cumplimiento de normativa en materia de niveles máximos de emisión.

3. La modificación los títulos habilitantes para el uso del dominio público radioeléctrico que hubiesen sido otorgados por el procedimiento de licitación se producirá mediante orden del Ministro de Energía, Turismo y Agenda Digital, con arreglo a los principios de objetividad, transparencia y proporcionalidad y atendiendo a los criterios señalados en el apartado anterior, previo informe de la Comisión Nacional de los Mercados y la Competencia y de la Comisión Delegada del Gobierno para Asuntos Económicos, previa consulta al Consejo de Consumidores y Usuarios, y previo trámite de audiencia a los interesados, estableciéndose un plazo suficiente para que remitan sus alegaciones que, salvo circunstancias excepcionales, no podrá ser inferior a cuatro semanas.

4. Los daños y perjuicios que se deriven de la modificación del título habilitante para el uso del dominio público radioeléctrico otorgado por el procedimiento de licitación llevada a cabo por el Ministerio de Energía, Turismo y Agenda Digital, sin mediar causa imputable a su titular, darán derecho a indemnización de acuerdo con los principios y reglas indemnizatorias de carácter general, salvo cuando venga impuesta por normas internacionales o por el ordenamiento jurídico de la Unión Europea.

5. La modificación de los títulos habilitantes para el uso del dominio público radioeléctrico, en los casos en que justificadamente haya que establecer condiciones distintas a las que existían cuando se otorgó el título, podrá consistir en prolongar la duración de derechos ya existentes, incluso más allá de las duraciones establecidas en el artículo 89, en cuyo caso dicha prolongación podrá entenderse que forma parte de la indemnización a la que se refiere el apartado anterior.

Artículo 91. *Reasignación del uso de bandas de frecuencias.*

1. Se entenderá por reasignación de uso de una determinada banda de frecuencias, su atribución a nuevos servicios de radiocomunicaciones o su explotación mediante tecnologías distintas a las utilizadas hasta ese momento. Serán causas justificativas de la reasignación de uso de una determinada banda de frecuencias, las siguientes:

a) Cumplimiento de la normativa comunitaria en materia de armonización del uso del espectro radioeléctrico.
b) Necesidad de utilización de la banda de frecuencias en cuestión para el despliegue de servicios de interés público, tanto si se trata de nuevos servicios como de ampliación de la capacidad de los ya existentes.
c) Introducción de nuevas tecnologías que aporten una mayor eficiencia espectral en la explotación de la banda de frecuencias.

2. Corresponde a la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital la identificación de las situaciones en las que resulta necesaria la reasignación de uso de una determinada banda de frecuencias, en base a las causas mencionadas en el apartado 1. Esta identificación podrá basarse también en las conclusiones de consultas públicas, constatación de espectro radioeléctrico insuficiente para atender la demanda planteada o informes de organismos o instituciones relacionadas con la competencia, la prestación de servicios de interés público o de operadores en general.

Artículo 92. *Procedimiento para la reasignación de bandas de frecuencias.*

1. El procedimiento para la reasignación de uso de una determinada banda de frecuencias con el objetivo de alcanzar un uso más eficiente del espectro radioeléctrico, se iniciará en todos los casos mediante la correspondiente modificación del Cuadro Nacional de Atribución de Frecuencias (CNAF), previo informe de la Comisión Nacional de los Mercados y la Competencia y de la Comisión Delegada del Gobierno para Asuntos Económicos, previa consulta al Consejo de Consumidores y Usuarios, y previo trámite de audiencia a los interesados, estableciéndose un plazo suficiente para que remitan sus alegaciones que, salvo circunstancias excepcionales, no podrá ser inferior a cuatro semanas, y sin perjuicio de otras disposiciones que puedan ser necesarias.
2. Cuando la reasignación se produzca por el cumplimiento de la normativa europea, se introducirán en el Cuadro Nacional de Atribución de Frecuencias los cambios necesarios para habilitar dicha banda de frecuencias para la prestación de los nuevos servicios en los plazos establecidos en las disposiciones comunitarias.
3. Cuando la reasignación de uso se produzca por necesidades de espectro para servicios de interés general o por la introducción de nuevas tecnologías el procedimiento se iniciará de oficio por la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital.
4. Efectuada la modificación del Cuadro Nacional de Atribución de Frecuencias, el procedimiento para la reasignación de bandas de frecuencias continuará con la modificación de los títulos habilitantes para el uso del dominio público radioeléctrico afectados, en conformidad con lo dispuesto en el artículo 90.

Artículo 93. *Renovación de los títulos habilitantes en el caso de uso especial del espectro en el caso de autorizaciones generales y de uso privativo del dominio público radioeléctrico sin limitación de número de titulares.*

1. La renovación de los títulos habilitantes en el caso de uso especial del espectro en el caso de autorizaciones generales y de uso privativo del dominio público radioeléctrico sin limitación de número de titulares se efectuará de oficio a la finalización de cada uno de sus periodos de vigencia.
2. En el caso de que el titular no desee la renovación de oficio de su título habilitante para el uso del dominio público radioeléctrico, deberá comunicarlo a la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital con una antelación mínima de tres meses a la fecha de finalización del periodo de vigencia del título.

3. Conjuntamente con el procedimiento de renovación, podrá tramitarse un procedimiento de modificación del título habilitante para el uso del dominio público radioeléctrico cuando concurran las circunstancias señaladas en el apartado 2 del artículo 90. El titular dispondrá de un plazo de quince días para manifestar la no aceptación de las citadas modificaciones en cuyo caso se dictaría resolución de extinción del título. En caso contrario se entenderá que el titular acepta las modificaciones propuestas, y el título habilitante para el uso del dominio público radioeléctrico quedaría renovado con las citadas modificaciones.

No darán derecho a indemnización las modificaciones que se produzcan con ocasión de cualquiera de las renovaciones que, en su caso, se otorguen, siempre que estas modificaciones resulten necesarias de acuerdo con lo establecido en el artículo 90.

4. Con anterioridad a la finalización del periodo de vigencia del título habilitante para el uso del dominio público radioeléctrico, la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital dictará resolución sobre la renovación del título, y la notificará a los titulares de los derechos de uso. Dicha resolución podrá consistir en:

a) La renovación del título habilitante para el uso del dominio público radioeléctrico sin modificación, cuando el titular no hubiera renunciado a la renovación y no fuera necesario modificar el título.

b) La renovación del título habilitante para el uso del dominio público radioeléctrico con modificación, cuando el titular hubiera aceptado la modificación de las condiciones del título, propuesta por la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital.

c) La extinción del título habilitante para el uso del dominio público radioeléctrico cuando el titular hubiera renunciado a la renovación, cuando el titular no hubiera aceptado su modificación, o cuando no resulte posible la modificación del título para su adaptación a las circunstancias enunciadas en el apartado 2 del artículo 90.

5. Si al concluir el período de vigencia del título, la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital no hubiera dictado resolución sobre la renovación del título habilitante para el uso del dominio público radioeléctrico, el titular podrá seguir utilizando el dominio público radioeléctrico en las condiciones establecidas en el título original, hasta que dicha Secretaría de Estado dicte resolución expresa.

6. En caso de que no se produzca la renovación del título, éste se entenderá extinguido desde la fecha de finalización de su periodo de vigencia.

Artículo 94. *Extinción de los títulos habilitantes para el uso del dominio público radioeléctrico.*

1. Los títulos habilitantes para el uso del dominio público se extinguirán por las siguientes causas:

a) Las causas que resulten aplicables de las reseñadas en el artículo 100 de la Ley 33/2003, de 3 de noviembre, de Patrimonio de las Administraciones Públicas.

b) Muerte del titular del derecho de uso del dominio público radioeléctrico o extinción de la persona jurídica titular.

c) Renuncia del titular, con efectos desde su aceptación por el órgano competente del Ministerio de Energía, Turismo y Agenda Digital.

d) Pérdida de la condición de operador del titular del derecho de uso del dominio público radioeléctrico, cuando dicha condición fuera necesaria, o por cualquier causa que imposibilite la prestación del servicio por su titular.

e) Falta de pago de la tasa por reserva del dominio público radioeléctrico.

f) Pérdida de adecuación de las características técnicas de la red radioeléctrica al Cuadro Nacional de Atribución de Frecuencias, sin que exista posibilidad de modificar las condiciones técnicas de red radioeléctrica o de autorizar al titular el uso de otras bandas de frecuencia.

g) Mutuo acuerdo entre el titular y el órgano competente del Ministerio de Energía, Turismo y Agenda Digital.

h) Transcurso del tiempo para el que se otorgaron. En el caso de los derechos de uso sin limitación de número, por el transcurso del tiempo para el que se otorgaron, sin que se haya efectuado su renovación.

i) Por incumplimiento grave y reiterado de las obligaciones del titular, contempladas como causa de revocación.

j) Aquellas otras causas que se establezcan en el título habilitante para el uso del dominio público radioeléctrico.

2. Una vez extinguido el título habilitante para el uso del dominio público radioeléctrico, deberá procederse al cese inmediato de las emisiones desde la fecha de notificación de la resolución que acuerde la extinción de dicho título habilitante.

Artículo 95. *Revocación de los títulos habilitantes para el uso del dominio público radioeléctrico.*

1. El órgano competente del Ministerio de Energía, Turismo y Agenda Digital, de oficio, a través del procedimiento administrativo común de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, podrá acordar la revocación de los títulos habilitantes para el uso del dominio público radioeléctrico por las siguientes causas:

a) Incumplir las condiciones y requisitos técnicos o administrativos aplicables al uso del dominio público radioeléctrico, en particular no respetar las servidumbres radioeléctricas, los límites que se hubieran establecido en relación con la cantidad de espectro que podrá ser reservado en favor de un mismo titular, o la normativa en materia de niveles máximos de emisión.

b) No pagar, cuando proceda, el Impuesto de Transmisiones Patrimoniales y Actos Jurídicos Documentados.

c) No efectuar un uso eficaz o eficiente del dominio público radioeléctrico.

d) Revocación de dos autorizaciones administrativas de cesión de derechos de uso del dominio público radioeléctrico sobre el mismo título habilitante, en el plazo de un año.

e) Utilizar las frecuencias con fines distintos a los que motivaron su asignación o para otros usos diferentes a los de la prestación del servicio o el ejercicio de la actividad que haya motivado su asignación.

2. Una vez revocado el título habilitante para el uso del dominio público radioeléctrico, deberá procederse al cese inmediato de las emisiones desde la fecha de notificación de la resolución que acuerde la revocación de dicho título habilitante.

TÍTULO VIII

Inspección y control del dominio público radioeléctrico

CAPÍTULO I

Inspección de telecomunicaciones

Artículo 96. *Facultades del personal de inspección del dominio público radioeléctrico.*

1. De acuerdo con lo establecido en el artículo 73 de la Ley General de Telecomunicaciones, los funcionarios destinados en la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital del Ministerio de Energía, Turismo y Agenda Digital tienen, en el ejercicio de sus funciones inspectoras en materia de telecomunicaciones, la consideración de autoridad pública y podrán solicitar, a través de la autoridad gubernativa correspondiente, el apoyo necesario de los Cuerpos y Fuerzas de Seguridad.

2. En particular, tendrán la consideración de autoridad pública todos los funcionarios destinados en la Subdirección General de Inspección de las Telecomunicaciones o en las Jefaturas Provinciales de Inspección de Telecomunicaciones que realicen las siguientes funciones inspectoras:

a) La inspección de los servicios y de las redes de comunicaciones electrónicas, incluidas sus condiciones de prestación y explotación, así como la inspección de equipos, aparatos e instalaciones de los sistemas civiles.

b) El control de los niveles de calidad en la explotación de redes y prestación de servicios de comunicaciones electrónicas.

c) El control y la inspección de instalaciones y estaciones que utilizan el dominio público radioeléctrico.

d) La comprobación técnica de emisiones radioeléctricas para la identificación, localización y eliminación de interferencias perjudiciales, infracciones, irregularidades y perturbaciones de los sistemas de radiocomunicación.

e) El control de los niveles de exposición radioeléctrica causados por equipos, aparatos e instalaciones de los sistemas civiles.

f) Las actuaciones relacionadas con la evaluación de la conformidad de equipos y aparatos radioeléctricos y demás actuaciones derivadas de su puesta en el mercado.

3. Los funcionarios que ejercen funciones inspectoras en materia de telecomunicaciones dispondrán de una tarjeta de identificación que les acredite como inspectores de telecomunicación.

4. Los funcionarios de la inspección de telecomunicaciones podrán recabar cuantas informaciones precisen para el cumplimiento de sus cometidos. Las personas físicas o jurídicas que puedan tener alguna información relacionada con el objeto de una inspección de telecomunicaciones tienen la obligación de comunicarla.

A tal efecto, dichos funcionarios podrán solicitar la exhibición o el envío de documentos y datos o examinarlos en el lugar en que se encuentren depositados, así como inspeccionar los equipos físicos y lógicos utilizados para las comunicaciones, accediendo a los locales donde se hallen instalados.

5. Los funcionarios de la inspección de telecomunicaciones, en el ejercicio de la función inspectora, podrán ser asistidos por otro personal técnico, cuando así lo consideren necesario, pudiendo ser acompañados por ellos en las inspecciones que realicen a terceros.

6. Los funcionarios de la inspección de telecomunicaciones, así como otro personal de inspección colaborador, en el ejercicio de sus funciones, tienen la facultad de entrar en las instalaciones de telecomunicación para llevar a cabo el control de los elementos afectos a los servicios o actividades que realicen, de las redes y estaciones que instalen o exploten, y de cuantos documentos están obligados a poseer o conservar.

La falta de consentimiento del titular, o del responsable, para el acceso a las instalaciones, a fincas o a bienes inmuebles, así como la negativa para facilitar la información o documentación que sea requerida será considerada como una obstrucción a ser inspeccionado y falta de colaboración con la inspección de telecomunicaciones.

7. Las unidades móviles de la inspección de telecomunicaciones, en el ejercicio de las funciones inspectoras, son vehículos oficiales destinados a la prestación del servicio público de inspección de telecomunicaciones y, en particular, en el procedimiento de determinación, control e inspección de los niveles de exposición radioeléctrica para garantizar que no supongan un peligro para la salud pública.

8. Los servicios técnicos del Ministerio de Energía, Turismo y Agenda Digital elaborarán planes de inspección para comprobar la adaptación de las estaciones radioeléctricas a lo dispuesto en este reglamento. Con carácter anual, dicho ministerio, sobre la base de los resultados obtenidos en las citadas inspecciones y de las certificaciones presentadas por los operadores, elaborará y hará público un informe sobre la exposición a emisiones radioeléctricas.

Artículo 97. *Acceso a las instalaciones de telecomunicación.*

1. Los titulares de derechos de uso del dominio público radioeléctrico, los prestadores de servicios de radiocomunicaciones, los operadores de telecomunicaciones, los titulares de las estaciones radioeléctricas, las empresas instaladoras o mantenedoras de las instalaciones, quienes hagan uso del espectro radioeléctrico, y los titulares de fincas o bienes inmuebles están obligados a facilitar y permitir al personal de inspección, en el ejercicio de sus

funciones inspectoras en materia de telecomunicaciones, el acceso a sus instalaciones y la inspección de las estaciones.

2. En el caso de que las citadas personas, físicas o jurídicas, se opusieran a facilitar y permitir el acceso de los funcionarios de inspección a sus instalaciones no situadas en domicilios constitucionalmente protegidos y, en particular, en instalaciones de telecomunicación situadas fuera de los núcleos de población, con caseta para equipos donde no residen habitualmente personas ni constituye el centro de toma de decisiones de una empresa, mediante resolución del Director General de Telecomunicaciones y Tecnologías de la Información podrá ordenarse a las citadas personas que se sometan a la inspección y faciliten el acceso a dichas instalaciones.

3. Cuando el acceso a las instalaciones, o el registro en las mismas, afecte al domicilio constitucionalmente protegido se precisará el consentimiento de los titulares de la correspondiente finca o inmueble, o una autorización judicial. En este último caso, se solicitará el acceso a un emplazamiento radioeléctrico o a un emplazamiento radioeléctrico equivalente, que no tiene que coincidir con un único emplazamiento físico.

Artículo 98. *Información relacionada con las instalaciones de telecomunicación.*

1. Los titulares de derechos de uso del dominio público radioeléctrico, los prestadores de servicios de radiocomunicaciones, los operadores de telecomunicaciones, los titulares de las estaciones radioeléctricas, las empresas instaladoras o mantenedoras de las instalaciones donde se ubiquen las instalaciones, equipos y aparatos de telecomunicaciones, quienes hagan uso del espectro radioeléctrico, los titulares de fincas o bienes inmuebles, las empresas suministradoras de electricidad, el consumidor, el usuario final y quienes estén relacionados con las comunicaciones están obligados a someterse a las inspecciones y a poner a disposición del personal de inspección cuantos libros, registros, documentos y medios técnicos, incluidos los programas informáticos y los archivos magnéticos, ópticos o de cualquier otra clase que se consideren precisos.

En particular, las empresas suministradoras del fluido eléctrico o del agua están obligadas a facilitar los nombres y direcciones de los titulares que constan en un determinado emplazamiento radioeléctrico.

2. Asimismo, deberán facilitar cualquier tipo de documentación que el personal de la inspección les exija para la determinación de la titularidad de los equipos o la autoría de emisiones o actividades.

3. Las obligaciones anteriores también serán exigibles a quienes den soporte a las actividades objeto de inspección, así como a las asociaciones de empresas y a los administradores y otros miembros del personal de todas ellas.

CAPÍTULO II

Uso adecuado del dominio público radioeléctrico

Artículo 99. *Emisiones que perjudican o vulneran los planes de utilización del dominio público radioeléctrico o el Cuadro Nacional de Atribución de Frecuencias.*

1. Se considerarán emisiones que vulneran o perjudican el Cuadro Nacional de Atribución de Frecuencias aquellas que no sean conformes con una o varias de las características y requisitos establecidos en el mismo.

2. Las emisiones radioeléctricas no autorizadas que produzcan una intensidad de campo en una zona de servicio de una estación establecida en un plan, o de una red de estaciones, superior a la intensidad de campo admisible, se considerará que perjudican o vulneran dicho plan de utilización del dominio público radioeléctrico. La intensidad de campo admisible es la diferencia entre la intensidad de campo a proteger y la correspondiente relación de protección. Las intensidades de campo a proteger y las relaciones de protección aplicables son las establecidas por la normativa nacional o, en su defecto, por las normas técnicas o recomendaciones aprobadas por los organismos internacionales competentes.

3. Igualmente, se considerará que perjudican o vulneran un plan de utilización del dominio público radioeléctrico las emisiones que no respeten las condiciones de protección establecidas en dicho plan, o que no respeten los parámetros establecidos en el mismo.

Artículo 100. *Interferencias perjudiciales sobre el servicio prestado por una estación autorizada.*

1. En los servicios de cobertura zonal, la existencia de interferencia perjudicial, conforme ha sido definida en el apartado 20 del anexo II de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, sobre el servicio prestado por una estación radioeléctrica, quedará verificada siempre que la intensidad de campo interferente supere la intensidad de campo admisible. La intensidad de campo admisible es la diferencia entre la intensidad de campo a proteger y la correspondiente relación de protección. Las intensidades de campo a proteger y las relaciones de protección aplicables son las establecidas por la normativa nacional o, en su defecto, por las normas técnicas o recomendaciones aprobadas por los organismos internacionales competentes.

2. En los servicios punto a punto, la existencia de interferencia perjudicial, conforme ha sido definida en el apartado 20 del anexo II de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, sobre el servicio prestado por una estación radioeléctrica, quedará verificada siempre que la potencia de la señal interferente supere la diferencia entre la potencia a proteger y la relación de protección.

3. En todo caso, existe interferencia perjudicial, conforme ha sido definida en el apartado 20 del anexo II de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, cuando la señal interferente no respete la relación de protección establecida en la normativa nacional o, en su defecto, por las normas técnicas o recomendaciones aprobadas por los organismos internacionales competentes.

Artículo 101. *Derecho a la protección frente a interferencias.*

1. Tienen derecho a protección frente a interferencias perjudiciales, causadas por cualquier otra estación o equipo, los titulares habilitados para el uso del dominio público radioeléctrico que lo utilicen en las condiciones autorizadas en el correspondiente título o, en su caso, en las condiciones establecidas en el Cuadro Nacional de Atribución de Frecuencias, y dispongan de la autorización para la puesta en servicio cuando resulte exigible. Esta protección se asegurará en los términos establecidos en el presente reglamento y en el Cuadro Nacional de Atribución de Frecuencias.

2. Dichos titulares podrán reclamar la correspondiente protección ante la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital.

Artículo 102. *Solicitud de intervención ante interferencias.*

Sin perjuicio de los protocolos de actuación que se puedan establecer entre los servicios técnicos de la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital y determinados titulares habilitados para el uso del dominio público radioeléctrico que, por sus especiales características, se considere necesario tratar de forma específica, la solicitud de intervención ante interferencias se ajustará al modelo que se publicará en la sede electrónica del Ministerio de Energía, Turismo y Agenda Digital, incluyendo el máximo de datos posible que puedan contribuir a identificar el origen y las características de la interferencia. Dicha solicitud se dirigirá a la Jefatura Provincial de Inspección de Telecomunicaciones correspondiente a la provincia en la que se produzca la interferencia o donde se sitúe la estación interferente.

Artículo 103. *Tratamiento de las interferencias peligrosas.*

1. La interferencia peligrosa es la interferencia perjudicial que se produce sobre un servicio de radiocomunicación asociado a la seguridad de vidas humanas.

2. El tratamiento de las interferencias peligrosas tiene prioridad sobre el resto de interferencias y, sin perjuicio de las sanciones que puedan corresponder, se podrán aplicar las medidas previstas en el artículo 81 de la Ley General de Telecomunicaciones.

Artículo 104. *Retirada de elementos transmisores de las estaciones radioeléctricas.*

El titular del título habilitante para el uso del dominio público radioeléctrico que sea objeto de extinción o revocación, de acuerdo con lo previsto en los artículos 94 y 95 de este

reglamento, será responsable de la retirada de los elementos transmisores de las estaciones radioeléctricas asociadas al mismo, en el plazo máximo de tres meses desde la fecha de notificación de la resolución que acuerde la extinción o revocación de dicho título habilitante.

Asimismo, el titular de una estación radioeléctrica que sea cancelada de oficio o previa solicitud, será responsable de la retirada de los elementos transmisores en el plazo máximo de tres meses desde la fecha de notificación de la resolución de cancelación.

Artículo 105. *Obligaciones después de la autorización para la puesta en servicio.*

1. Los titulares de derechos de uso del dominio público radioeléctrico deberán cumplir con las obligaciones adquiridas, y en particular con este reglamento y con el Reglamento que establece condiciones de protección del dominio público radioeléctrico, restricciones a las emisiones radioeléctricas y medidas de protección sanitaria frente a emisiones radioeléctricas, aprobado por el Real Decreto 1066/2001, de 28 de septiembre. En caso de no hacerlo, se considerará una falta grave incumplir con las condiciones de prestación de servicios establecidas, de acuerdo con el artículo 77.17 de la Ley General de Telecomunicaciones.

2. Los titulares de las estaciones correspondientes a las redes y servicios a que se refiere el apartado 1 del artículo 53, deberán remitir al Ministerio de Energía, Turismo y Agenda Digital, en el primer trimestre de cada año natural, una certificación realizada por un técnico competente de que se han respetado los límites de exposición establecidos en el anexo II del reglamento aprobado mediante el Real Decreto 1066/2001, de 28 de septiembre. Dicho ministerio podrá ampliar esta obligación a titulares de otras instalaciones radioeléctricas.

TÍTULO IX

Protección del dominio público radioeléctrico

CAPÍTULO I

Limitaciones y servidumbres para la protección del dominio público radioeléctrico

Artículo 106. *Limitaciones y servidumbres para la protección de determinadas instalaciones radioeléctricas.*

1. De conformidad con lo establecido en el artículo 33 de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, podrán establecerse las limitaciones a la propiedad y a la intensidad de campo eléctrico y las servidumbres que resulten necesarias para la protección radioeléctrica de determinadas instalaciones o para asegurar el adecuado funcionamiento de estaciones o instalaciones radioeléctricas utilizadas para la prestación de servicios públicos, por motivos de seguridad pública o cuando así sea necesario en virtud de acuerdos internacionales.

2. Los valores máximos de las limitaciones y servidumbres que resulten necesarias para la protección radioeléctrica de las instalaciones a que se refiere este artículo figuran en el anexo 2 de este reglamento.

3. Las servidumbres y limitaciones aeronáuticas se regirán por su normativa específica.

4. El presente Reglamento será de aplicación supletoria en los supuestos regulados en el Reglamento de la Ley 8/1975, de 12 de marzo, de zonas e instalaciones de interés para la Defensa Nacional, aprobado por el Real Decreto 689/1978, de 10 de febrero.

Artículo 107. *Concepto de limitaciones a la propiedad y servidumbres para la protección de determinadas instalaciones radioeléctricas.*

1. A efectos de lo dispuesto en el presente capítulo, se entenderá por limitación a la propiedad para la protección radioeléctrica de instalaciones, la obligación de no hacer y de soportar no individualizada, impuesta a los titulares y propietarios de los predios cercanos a las estaciones o instalaciones objeto de la protección.

Asimismo, de acuerdo con el artículo 33 de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, se entenderá por servidumbre la obligación de no hacer y de soportar de carácter individualizado, indemnizable en los términos de la legislación de expropiación forzosa. Igualmente, las limitaciones a la propiedad, cuando efectivamente causen una privación singular, serán indemnizables con arreglo a lo dispuesto en la legislación sobre expropiación forzosa.

2. Los propietarios no podrán realizar obras o modificaciones en los predios sirvientes que impidan dichas servidumbres o limitaciones, una vez que las mismas se hayan constituido, según lo previsto en el artículo siguiente de este reglamento.

3. La constitución de dichas servidumbres y limitaciones deberá reducir en lo posible el gravamen que las mismas impliquen y someterse a las reglas de congruencia y proporcionalidad.

Artículo 108. *Constitución de limitaciones y servidumbres.*

1. Los expedientes de constitución de las limitaciones que no causen una privación singular, se iniciarán por la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital, de oficio o a instancia de parte, y contendrán, como mínimo, la motivación de su necesidad, su ámbito geográfico y su alcance.

2. Dichos expedientes se someterán a las reglas de publicidad, de igualdad de trato y de generalidad de la limitación y se someterán al trámite de audiencia previsto en el artículo 82 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. No obstante, se podrá omitir este trámite de audiencia en ausencia de interesados conocidos. En todo caso, se publicará un extracto en el «Boletín Oficial del Estado» para información pública, otorgándose un plazo de veinte días para la presentación de alegaciones.

3. Concluida la tramitación del expediente administrativo, el Ministro de Energía, Turismo y Agenda Digital, a propuesta de la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital, y previo informe de la Abogacía del Estado en el Departamento, resolverá sobre dicho expediente.

4. La orden de aprobación de la limitación se publicará en el «Boletín Oficial del Estado» y se notificará a los interesados en los términos previstos en el artículo 41 y siguientes de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

5. Los expedientes para la constitución de las servidumbres y de las limitaciones que efectivamente causen una privación singular, se iniciarán por la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital, de oficio o a instancia de parte, y se regirán por lo dispuesto en la legislación sobre expropiación forzosa.

CAPÍTULO II

Protección activa del dominio público radioeléctrico

Artículo 109. *Protección activa del dominio público radioeléctrico.*

1. La Secretaría de Estado para la Sociedad de la Información y la Agenda Digital, en cualquier momento, podrá efectuar una protección activa del dominio público radioeléctrico mediante la realización de emisiones sin contenidos sustantivos en aquellas frecuencias y canales radioeléctricos cuyos derechos de uso, en el ámbito territorial correspondiente, no hayan sido otorgados.

2. Esta potestad se ejercitará sin perjuicio de las actuaciones inspectoras y sancionadoras que se puedan llevar a cabo para depurar las responsabilidades en que se hubiera podido incurrir por el uso del dominio público radioeléctrico sin disponer de título habilitante, por la producción de interferencias perjudiciales o por la comisión de cualquier otra infracción tipificada en el marco del régimen sancionador establecido en el Título VIII de la Ley General de Telecomunicaciones.

3. Será de aplicación el ejercicio de la potestad de protección activa del dominio público radioeléctrico en el caso de que la frecuencia o canal radioeléctrico sea objeto de una

ocupación o uso efectivo sin que se disponga de título habilitante para el uso del dominio público radioeléctrico, con sujeción a las siguientes normas:

a) Los servicios técnicos de la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital constatarán la ocupación o uso efectivo de la frecuencia o canal radioeléctrico sin que se disponga de título habilitante para ello.

b) Se efectuará un trámite de audiencia previa a la persona física o jurídica que esté efectuando la ocupación o el uso de la frecuencia o canal radioeléctrico sin título habilitante para el uso del dominio público radioeléctrico o, en su caso si este resultase ilocalizable, al titular de las infraestructuras, de la finca o del inmueble desde donde se produce la emisión en esa frecuencia, para que en el plazo de diez días hábiles alegue lo que estime oportuno.

c) En su caso, una vez efectuado el trámite de audiencia previa, se requerirá a la persona o titular mencionado anteriormente con el que se evacuó dicho trámite, para que en el plazo de ocho días hábiles se proceda al cese de las emisiones no autorizadas.

d) En el caso de que no se proceda al cese de las emisiones no autorizadas, la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital, de manera directa o a través de tercero, podrá iniciar sus emisiones en dicha frecuencia o canal radioeléctrico.

Disposición adicional primera. *Bandas de frecuencias con limitación de número de títulos habilitantes para el uso del dominio público radioeléctrico a otorgar.*

De conformidad con lo previsto en el apartado 3 del artículo 37, y sin perjuicio de su modificación por la persona titular del Ministerio de Asuntos Económicos y Transformación Digital, previo informe preceptivo de la Comisión Nacional de los Mercados y la Competencia, y previo acuerdo de la Comisión Delegada del Gobierno para Asuntos Económicos, la relación de bandas de frecuencias para redes terrestres en las que, por ser precisa la garantía del uso eficaz y eficiente del dominio público radioeléctrico, se limita el número de concesiones para su uso es, inicialmente, la siguiente:

a) 694 a 790 MHz.
b) 790 a 862 MHz.
c) 880 a 915 y 925 a 960 MHz.
d) 1.427 a 1.517 MHz.
e) 1.710 a 1.785 y 1.805 a 1.880 MHz.
f) 1.900 a 2.025 y 2.110 a 2.200 MHz.
g) 2.500 a 2.690 MHz.
h) 3,42 a 3,8 GHz.
i) 24,70 a 27,50 GHz.

Disposición adicional segunda. *Prestación de servicios móviles por satélite.*

El otorgamiento del título habilitante para el uso del dominio público radioeléctrico a los operadores seleccionados como idóneos para la prestación de servicios móviles por satélite de acuerdo al procedimiento establecido en la Decisión 626/2008/CE del Parlamento Europeo y del Consejo, de 30 de junio de 2008, relativa a la selección y autorización de sistemas que prestan servicios móviles por satélite y la Decisión 2009/449/CE, de la Comisión, de 13 de mayo de 2009, relativa a la selección de operadores de sistemas paneuropeos que prestan servicios móviles por satélite, así como las condiciones de autorización de las estaciones complementarias en tierra se regirá por lo establecido en las Decisiones antes citadas, en la Ley General de Telecomunicaciones y en el presente reglamento.

ANEXO 1

Servicios con frecuencias reservadas en las bandas indicadas susceptibles de cesión a terceros de los derechos de uso del dominio público radioeléctrico

Servicios	Bandas
Servicios móviles en régimen de autoprestación. (Redes privadas (PMR y otros).	68-87,5 MHz 146-174 MHz 223-235 MHz 406,1-430 MHz 440-470 MHz 870-876/915-921 MHz 24,25-24,70 GHz
Servicios de comunicaciones electrónicas (Redes públicas).	68-87,5 MHz 146-174 MHz 223-235 MHz 406,1-430 MHz 440-470 MHz 790-862 MHz 870-876/915-921 MHz 880-915/925-960 MHz 1452-1492 MHz 1710-1785/1805-1880 MHz 1900-1920 MHz 1920-1980/2110-2170 MHz 2010-2025 MHz 3420-3800 MHz 2500-2690 MHz 24,70-27,50 GHz 28332,5-28444,5/29340,5-29452,5 MHz
Servicio fijo (Redes privadas).	1.427-1.452/1.492-1.518 MHz 1.525-1.530 MHz 2.025-2.110/2.200-2290 MHz 2.290-2.300 MHz 3.600-4.200 MHz 4.500-.000 MHz 5,9-6,4/6,4-7,1 GHz 7,725-7,975 GHz/8,025-8,275 GHz 10,449-10,680 GHz 12,75-13,25 GHz 14,47 - 14,753/14,865-15,173 GHz 15,285-15,350 GHz 17,7-19,7 GHz 21,2-21,4 GHz 22,0-22,6/23,0-23,6 GHz 27,9405-28,4445/28,9485-29,4525 GHz 27,8285-27,9405 GHz 31,0-31,3 GHz 37,0-39,5 GHz 40,5-47 GHz

ANEXO 2

Limitaciones y servidumbres para la protección de determinadas instalaciones radioeléctricas

1. De acuerdo con lo establecido en la disposición adicional segunda de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, se establecen tres tipos de limitaciones y servidumbres para la protección radioeléctrica o para asegurar el adecuado funcionamiento de las estaciones o instalaciones radioeléctricas a las que hace referencia el artículo 33 de la citada ley, que podrán afectar:

a) A la altura máxima de los edificios. Para distancias inferiores a 1.000 metros, el ángulo sobre la horizontal con el que se observe, desde la parte superior de las antenas receptoras de menor altura de la estación, el punto más elevado de un edificio será como máximo de tres grados.

b) A la distancia mínima a la que podrán ubicarse industrias que produzcan emisiones radioeléctricas e instalaciones eléctricas de alta tensión y líneas férreas electrificadas no soterradas. La máxima limitación exigible de separación entre una industria o una línea de tendido eléctrico de alta tensión o de ferrocarril y cualquiera de las antenas receptoras de la estación a proteger será de 1.000 metros.

c) A la distancia mínima a la que podrán instalarse transmisores radioeléctricos, con o sin condiciones radioeléctricas exigibles (CRE). Para determinados servicios de radiocomunicación se podrá optar entre mantener las distancias mínimas establecidas sin CRE o reducir estas distancias con las CRE necesarias.

En el siguiente cuadro se establecen las limitaciones máximas exigibles en distancia entre las antenas transmisoras de estaciones radioeléctricas y las antenas receptoras de la estación a proteger:

Gama de frecuencias (f)	Servicio perturbador	Rango de potencia radiada aparente (P) del transmisor en dirección a la estación a proteger	Distancia mínima entre la antena del transmisor y la estación a proteger	
f ≤ 30 MHz	Radiodifusión	0,01 kW < P ≤ 1 kW	2 km	
		1 kW < P ≤ 10 kW	10 km	
		10 kW < P	20 km	
	Otros servicios	0,01 kW < P ≤ 1 kW	2 km	1 km con CRE
		1 kW < P	10 km	5 km con CRE
30 MHz < f ≤ 3 GHz	Radiodifusión Radiolocalización Investigación espacial (T-e)	0,01 kW < P ≤ 1 kW	1 km	
		1 kW < P ≤ 10 kW	2 km	
		10 kW < P	5 km	
	Otros servicios	0,01 kW < P ≤ 1 kW	1 km	0,3 km con CRE
		1 kW < P	2 km	1 km con CRE
3 GHz < f	Radiolocalización Investigación espacial (T-e)	0,001 kW < P ≤ 1 kW	1 km	
		1 kW < P ≤ 10 kW	2 km	
		10 kW < P	5 km	
	Otros servicios	0,001 kW < P	1 km	0,2 km con CRE

Las condiciones radioeléctricas exigibles (CRE) serán aquellas condiciones técnicas y de apantallamiento o protección que deban incluirse en las estaciones radioeléctricas a fin de que sus emisiones no perturben el normal funcionamiento de la estación a proteger.

En caso de existir controversia sobre el grado de perturbación admisible, la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital establecerá la suficiencia o insuficiencia de las CRE.

En los casos de estaciones de comprobación técnica de emisiones, para el establecimiento de las CRE, dentro de las distancias mínimas establecidas en el cuadro anterior, se tendrán en cuenta, además, los límites siguientes establecidos en la Recomendación UIT-R SM-575:

Frecuencia fundamental (f)	Norma de intensidad de campo	Media cuadrática para más de una intensidad de campo fundamental
9 kHz ≤ f < 174 MHz	10 mV/m	30 mV/m
174 MHz ≤ f < 960 MHz	50 mV/m	150 mV/m

El valor de la media cuadrática de la intensidad de campo se aplica a señales múltiples pero, únicamente, cuando todas ellas están dentro de la banda de paso de RF del receptor de comprobación técnica.

2. La Secretaría de Estado para la Sociedad de la Información y la Agenda Digital podrá autorizar que se supere la altura máxima y se reduzcan las distancias mínimas a las que se refiere el apartado anterior, siempre y cuando se garantice el adecuado funcionamiento de las estaciones o instalaciones radioeléctricas a proteger.

3. Por lo que respecta a las limitaciones de intensidad de campo eléctrico en las estaciones de alta sensibilidad dedicadas a la investigación en los campos de radioastronomía y astrofísica, estas limitaciones serán las siguientes:

a) Las estaciones dedicadas a observaciones radioastronómicas, en cada una de las bandas de frecuencias que se encuentran atribuidas al servicio de radioastronomía en conformidad con el Cuadro Nacional de Atribución de Frecuencias, estarán protegidas contra la interferencia perjudicial por los niveles de intensidad de campo que se indican a continuación:

Intensidad de campo	Banda de frecuencias
-34,2 dB(µV/m)	1400 a 1427 MHz
-35,2 dB(µV/m)	1610,6 a 1613,8 MHz
-35,2 dB(µV/m)	1660 a 1670 MHz
-31,2 dB(µV/m)	2690 a 2700 MHz
-25,2 dB(µV/m)	4990 a 5000 MHz
-14,2 dB(µV/m)	10,6 a 10,7 GHz
-10,2 dB(µV/m)	15,35 a 15,4 GHz
-2,2 dB(µV/m)	22,21 a 22,5 GHz
-1,2 dB(µV/m)	23,6 a 24 GHz
4,8 dB(µV/m)	31,3 a 31,8 GHz
8,8 dB(µV/m)	42,5 a 43,5 GHz
15,8 dB(µV/m)	76 a 77,5 GHz
16,8 dB(µV/m)	79 a 86 GHz
20,8 dB(µV/m)	86 a 94 GHz
21,8 dB(µV/m)	94,1 a 116 GHz
21,8 dB(µV/m)	130 a 134 GHz
21,8 dB(µV/m)	136 a 158,5 GHz
22,8 dB(µV/m)	164 a 167 GHz
24,8 dB(µV/m)	182 a 185 GHz
26,8 dB(µV/m)	200 a 231,5 GHz
27,8 dB(µV/m)	241 a 248 GHz
28,8 dB(µV/m)	250 a 275 GHz

b) Para la protección de las instalaciones de observatorios de astrofísica, la limitación de la intensidad de campo eléctrico, en cualquier frecuencia, será de 88,8 dB(µV/m) en la ubicación del observatorio. Para la determinación de la intensidad de campo se tendrán en cuenta las estaciones de radiocomunicaciones cuyas potencias radiadas aparentes en dirección a los observatorios sean superiores a 25 vatios y estén situadas en un círculo de 20 kilómetros de radio alrededor de la ubicación del observatorio de astrofísica o, en el caso de las Comunidades Autónomas insulares, las que estén situadas en la isla donde esté ubicado el observatorio.

Para los cálculos se tendrán en cuenta sus características técnicas y, en particular, las de la antena transmisora y las condiciones de apantallamiento del terreno y protección radioeléctrica. En el caso de que los cálculos teóricos den como resultado una intensidad de campo eléctrico superior al límite fijado, podrán realizarse medidas de intensidad de campo en la ubicación de los observatorios con señales de prueba.

4. Para un mejor aprovechamiento del espectro radioeléctrico, el Ministerio de Energía, Turismo y Agenda Digital podrá imponer en las instalaciones la utilización de aquellos elementos técnicos que mejoren la compatibilidad radioeléctrica entre estaciones.

§ 42

Real Decreto 1066/2001, de 28 de septiembre, por el que se aprueba el Reglamento que establece condiciones de protección del dominio público radioeléctrico, restricciones a las emisiones radioeléctricas y medidas de protección sanitaria frente a emisiones radioeléctricas

Ministerio de la Presidencia
«BOE» núm. 234, de 29 de septiembre de 2001
Última modificación: 8 de marzo de 2017
Referencia: BOE-A-2001-18256

Desde la introducción de manera generalizada de los servicios de radiodifusión de televisión y de radio, hace ya varias décadas, los ciudadanos han disfrutado en su vida cotidiana de los mismos, pero también se han visto sometidos inevitablemente a la exposición de campos electromagnéticos.

La introducción reciente de la competencia en el sector de las telecomunicaciones en España, se ha traducido en una mayor diversidad en la oferta de servicios de telecomunicaciones para empresas y ciudadanos, siendo esto particularmente apreciable en los servicios de telefonía móvil. Esta mayor diversidad de oferta de servicios de telecomunicaciones, y sus niveles de calidad y cobertura asociados, requiere la existencia de un elevado número de instalaciones radioeléctricas.

El Reglamento que se aprueba por este Real Decreto tiene, entre otros objetivos, adoptar medidas de protección sanitaria de la población. Para ello, se establecen unos límites de exposición del público en general a campos electromagnéticos procedentes de emisiones radioeléctricas, acordes con las recomendaciones europeas. Para garantizar esta protección se establecen unas restricciones básicas y unos niveles de referencia que deberán cumplir las instalaciones afectadas por este Real Decreto. Al mismo tiempo, se da respuesta a la preocupación expresada por algunas asociaciones, ciudadanos, corporaciones locales y Comunidades Autónomas.

El presente Real Decreto cumple con las propuestas contenidas en las mociones del Congreso de los Diputados y del Senado, que instaron al Gobierno a desarrollar una regulación relativa a la exposición del público en general a las emisiones radioeléctricas de las antenas de telefonía móvil.

Por otra parte, resulta también necesario, el establecimiento de condiciones que faciliten y hagan compatible un funcionamiento simultáneo y ordenado de las diversas instalaciones radioeléctricas y los servicios a los que dan soporte, considerándose, en particular, determinadas instalaciones susceptibles de ser protegidas.

El artículo 61 de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones establece que la gestión del dominio público radioeléctrico y las facultades para su administración y control corresponden al Estado. Además, este artículo añade que dicha gestión se ejercerá atendiendo a la normativa aplicable en la Unión Europea, y a las

resoluciones y recomendaciones de la Unión Internacional de Telecomunicaciones y de otros organismos internacionales.

El artículo 62 de la Ley 11/1998, establece, por su parte, que el Gobierno desarrollará reglamentariamente las condiciones de gestión del dominio público radioeléctrico, precisándose que en dicho Reglamento deberá incluirse el procedimiento de determinación de los niveles de emisión radioeléctrica tolerables y que no supongan un peligro para la salud pública.

El artículo 64, apartado 2, de la Ley 11/1998, dispone que se establecerán reglamentariamente, las limitaciones a la propiedad y las servidumbres, necesarias para la defensa del dominio público radioeléctrico, y para la protección radioeléctrica de las instalaciones de la Administración que se precisen para el control de la utilización del espectro.

El artículo 76 de la Ley 11/1998, establece que es competencia del Ministerio de Fomento (ahora, del Ministerio de Ciencia y Tecnología) la inspección de los servicios y de las redes de telecomunicaciones, de sus condiciones de prestación, de los equipos, de los aparatos, de las instalaciones y de los sistemas civiles, así como la aplicación del régimen sancionador, salvo que corresponda a la Comisión del Mercado de las Telecomunicaciones.

Adicionalmente, el Real Decreto 1451/2000, de 28 de julio, por el que se desarrolla la estructura orgánica básica del Ministerio de Ciencia y Tecnología, atribuye a la Dirección General de Telecomunicaciones y Tecnologías de la Información la competencia para la propuesta de planificación, gestión y administración del dominio público radioeléctrico, para la comprobación técnica de emisiones radioeléctricas, y para el control y la inspección de las telecomunicaciones, así como la aplicación del régimen sancionador en la materia.

La Ley 14/1986, de 25 de abril, General de Sanidad en sus artículos 18, 19, 24 y 40 atribuye a la administración sanitaria las competencias de control sanitario de los productos, elementos o formas de energía que puedan suponer un riesgo para la salud humana. Así mismo, atribuye la capacidad para establecer las limitaciones, métodos de análisis y requisitos técnicos para el control sanitario.

El Real Decreto 1450/2000, de 28 de julio, por el que se desarrolla la estructura orgánica básica del Ministerio de Sanidad y Consumo atribuye a la Dirección General de Salud Pública y Consumo la competencia para la evaluación, prevención y control sanitario de las radiaciones no ionizantes.

Para conseguir la protección efectiva de la salud pública es necesario coordinar las competencias del Ministerio de Ciencia y Tecnología, en relación con los límites de emisiones y gestión y protección del dominio público radioeléctrico, con las competencias sanitarias del Ministerio de Sanidad y Consumo.

Asimismo, resulta necesario que ambos Ministerios, con el fin de mejorar los conocimientos que se tienen acerca de la salud y las emisiones radioeléctricas promuevan y revisen la investigación pertinente sobre emisiones radioeléctricas y salud humana, en el contexto de sus programas de investigación nacionales, teniendo en cuenta las recomendaciones comunitarias e internacionales en materia de investigación y los esfuerzos realizados en este ámbito, basándose en el mayor número posible de fuentes.

El Reglamento que se aprueba por este Real Decreto, elaborado en coordinación por los Ministerios de Ciencia y Tecnología y de Sanidad y Consumo, tiene por objeto cumplir con lo establecido en los citados artículos de la Ley 11/1998, sobre emisiones radioeléctricas. Asimismo, el capítulo II, artículos 6 y 7, establece, con carácter de norma básica y en desarrollo de la Ley 14/1986, límites de exposición y condiciones de evaluación sanitaria de riesgos por emisiones radioeléctricas.

El presente Real Decreto asume los criterios de protección sanitaria frente a campos electromagnéticos procedentes de emisiones radioeléctricas establecidos en la Recomendación del Consejo de Ministros de Sanidad de la Unión Europea, de 12 de julio de 1999, relativa a la exposición del público en general a campos electromagnéticos.

Asimismo, esta Recomendación contempla la conveniencia de proporcionar a los ciudadanos información en un formato adecuado sobre los efectos de los campos electromagnéticos y sobre las medidas adoptadas para hacerles frente, al objeto de que se comprendan mejor los riesgos y la protección sanitaria contra la exposición a los mismos.

Este Reglamento establece unos límites de exposición, referidos a los sistemas de radiocomunicaciones, basados en la citada Recomendación del Consejo de la Unión Europea. Además, el Reglamento prevé mecanismos de seguimiento de los niveles de exposición, mediante la presentación de certificaciones e informes por parte de operadores de telecomunicaciones, la realización planes de inspección y la elaboración de un informe anual por parte del Ministerio de Ciencia y Tecnología.

El presente Real Decreto ha sido sometido a audiencia a través del Consejo Asesor de las Telecomunicaciones y de la Sociedad de la Información, y al informe de la Comisión del Mercado de las Telecomunicaciones, de acuerdo con lo previsto en el artículo 1, dos, 2, j) de la Ley 12/1997, de 24 de abril, de Liberalización de las Telecomunicaciones.

El presente Real Decreto ha sido sometido al procedimiento de información en materia de normas y reglamentaciones técnicas y de reglamentos relativos a los servicios de la Sociedad de la Información, previsto en la Directiva 98/34/CE, del Parlamento Europeo y del Consejo, de 22 de junio, modificada por la Directiva 98/48/CE, de 20 de julio, así como a lo previsto en el Real Decreto 1337/1999, de 31 de julio, por el que se regula la remisión de información en materia de normas y reglamentaciones técnicas y reglamentos relativos a los servicios de la sociedad de la información, que incorpora estas Directivas al ordenamiento jurídico español.

En su virtud, a propuesta conjunta de las Ministras de Ciencia y Tecnología y de Sanidad y Consumo, previa aprobación del Ministro de Administraciones Públicas, de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros en su reunión del día 28 de septiembre de 2001,

D I S P O N G O :

Artículo único. *Objeto.*

Mediante el presente Real Decreto se aprueba el Reglamento que establece condiciones de protección del dominio público radioeléctrico, restricciones a las emisiones radioeléctricas y medidas de protección sanitaria frente a emisiones radioeléctricas, que se incluye a continuación con los anexos que lo completan.

Disposición adicional única. *Elaboración de informes.*

Siguiendo la Recomendación 1999/519/CE del Consejo, de 12 de julio, relativa a la exposición del público en general a campos electromagnéticos, el Ministerio de Sanidad y Consumo elaborará, a los tres años de entrada en vigor de este Reglamento, un informe sobre las experiencias obtenidas en la aplicación del mismo, en lo referido a la protección frente a riesgos sanitarios potenciales de la exposición a las emisiones radioeléctricas.

Disposición derogatoria única. *Derogación normativa.*

Se deroga el capítulo II del título II del Reglamento de desarrollo de la Ley 31/1987, de 18 de diciembre, de Ordenación de las Telecomunicaciones, en relación con el dominio público radioeléctrico y los servicios de valor añadido que utilicen dicho dominio, aprobado por Real Decreto 844/1989, de 7 de julio.

Disposición final primera. *Desarrollo normativo y modificación de anexos.*

La Ministra de Ciencia y Tecnología dictará las disposiciones necesarias para el desarrollo y aplicación de este Real Decreto. Asimismo, se autoriza a la Ministra de Ciencia y Tecnología a modificar el anexo I del Reglamento, en función de la experiencia obtenida en su aplicación y de nuevas necesidades.

La Ministra de Sanidad y Consumo dictará las disposiciones necesarias para el desarrollo y aplicación de las funciones atribuidas al Ministerio de Sanidad y Consumo en este Real Decreto. Asimismo, se autoriza a la Ministra de Sanidad y Consumo a modificar el anexo II del Reglamento, de acuerdo con lo establecido en su artículo 7.

Disposición final segunda. *Fundamento legal y constitucional.*

Este Real Decreto se dicta en desarrollo de los artículos 48, 62 y 64 de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, dictada al amparo del artículo 149.1.21.ª de la Constitución, salvo la disposición adicional única y el capítulo II del Reglamento, artículos 6 y 7, que se dictan en desarrollo de los artículos 18, 19, 24 y 40 de la Ley 14/1986, de 25 de abril, General de Sanidad, con carácter de norma básica, en virtud del artículo 149.1.16.ª de la Constitución.

Disposición final tercera. *Entrada en vigor.*

Este Real Decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

REGLAMENTO QUE ESTABLECE CONDICIONES DE PROTECCIÓN DEL DOMINIO PÚBLICO RADIOELÉCTRICO, RESTRICCIONES A LAS EMISIONES RADIOELÉCTRICAS Y MEDIDAS DE PROTECCIÓN SANITARIA FRENTE A EMISIONES RADIOELÉCTRICAS

CAPITULO I

Disposiciones generales

Artículo 1. *Objeto.*

El presente Reglamento tiene por objeto el desarrollo de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, en lo relativo al establecimiento de condiciones de protección del dominio público radioeléctrico, a la autorización, planificación e inspección de instalaciones radioeléctricas en relación con los límites de exposición a las emisiones, el establecimiento de otras restricciones a las emisiones radioeléctricas, la evaluación de equipos y aparatos y el régimen sancionador aplicable. Asimismo, se desarrolla la Ley 14/1986, de 25 de abril, General de Sanidad, en relación con el establecimiento de límites de exposición para la protección sanitaria y la evaluación de riesgos por emisiones radioeléctricas.

Artículo 2. *Ámbito de aplicación.*

Las disposiciones de este Reglamento se aplican a las emisiones de energía en forma de ondas electromagnéticas, que se propagan por el espacio sin guía artificial, y que sean producidas por estaciones radioeléctricas de radiocomunicaciones o recibidas por estaciones del servicio de radioastronomía.

A los efectos de lo dispuesto en el párrafo anterior, se considera estación radioeléctrica uno o más transmisores o receptores, o una combinación de ambos, incluyendo las instalaciones accesorias, o necesarias para asegurar un servicio de radiocomunicación o el servicio de radioastronomía.

CAPITULO II

Protección del dominio público radioeléctrico

Artículo 3. *Limitaciones y servidumbres para la protección de determinadas instalaciones radioeléctricas.*

(Derogado)

Artículo 4. *Concepto de limitaciones a la propiedad y servidumbres para la protección de determinadas instalaciones radioeléctricas.*

(Derogado)

Artículo 5. *Constitución de limitaciones y servidumbres.*

(Derogado)

CAPITULO III

Límites de exposición para la protección sanitaria y evaluación de riesgos por emisiones radioeléctricas

Artículo 6. *Límites de exposición a las emisiones radioeléctricas. Restricciones básicas y niveles de referencia.*

En cumplimiento de lo dispuesto en el artículo 62 de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, y en desarrollo de la Ley 14/1986, de 25 de abril, General de Sanidad, de acuerdo con la Recomendación del Consejo de Ministros de Sanidad de la Unión Europea, de 12 de julio de 1999, y con el fin de garantizar la adecuada protección de la salud del público en general, se aplicarán los límites de exposición que figuran en el anexo II.

Los límites establecidos se cumplirán en las zonas en las que puedan permanecer habitualmente las personas y en la exposición a las emisiones de los equipos terminales, sin perjuicio de lo dispuesto en otras disposiciones específicas en el ámbito laboral.

Artículo 7. *Evaluación sanitaria de riesgos por emisiones radioeléctricas.*

En función de la evidencia científica disponible y de la información facilitada por el Ministerio de Ciencia y Tecnología, el Ministerio de Sanidad y Consumo, en coordinación con las Comunidades Autónomas, evaluará los riesgos sanitarios potenciales de la exposición del público en general a las emisiones radioeléctricas.

En la evaluación se tendrán en consideración el número de personas expuestas, sus características epidemiológicas, edad, partes del organismo expuestas, tiempo de exposición, condiciones sanitarias de las personas y otras variables que sean relevantes para la evaluación.

El Ministerio de Sanidad y Consumo, en coordinación con las Comunidades Autónomas, desarrollará los criterios sanitarios destinados a evaluar las fuentes y prácticas que puedan dar lugar a la exposición a emisiones radioeléctricas de la población, con el fin de aplicar medidas para controlar, reducir o evitar esta exposición. La aplicación de estas medidas se realizará en coordinación con el Ministerio de Ciencia y Tecnología.

Asimismo, el Ministerio de Sanidad y Consumo adaptará al progreso científico el anexo II, teniendo en cuenta el principio de precaución y las evaluaciones realizadas por las organizaciones nacionales e internacionales competentes.

CAPITULO IV

Autorización e inspección de instalaciones radioeléctricas en relación con los límites de exposición

Artículo 8. *Determinados requisitos para la autorización, criterios de planificación e instalación de estaciones radioeléctricas.*

(Derogado)

Artículo 9. *Inspección y certificación de las instalaciones radioeléctricas.*

(Derogado)

CAPITULO V

Otras disposiciones

Artículo 10. *Otras restricciones a los niveles de emisiones radioeléctricas.*

(Derogado)

Artículo 11. *Equipos y aparatos.*

(Derogado)

Artículo 12. *Instalación de estaciones radioeléctricas en un mismo emplazamiento.*

(Derogado)

Artículo 13. *Régimen sancionador.*

(Derogado)

Disposición transitoria única. *Certificación y señalización de instalaciones autorizadas.*

1. En el plazo de nueve meses, contado a partir de la entrada en vigor de este Reglamento, los operadores y titulares de licencias individuales a los que se refiere el apartado 1 del artículo 8, que dispongan de instalaciones radioeléctricas autorizadas con anterioridad a la fecha de entrada en vigor de este Reglamento, remitirán, al Ministerio de Ciencia y Tecnología, una certificación de la conformidad de dichas instalaciones con los límites de exposición establecidos en el anexo II de este Reglamento, expedida por técnico competente.

En caso de que transcurrido el citado plazo no se presentase la certificación correspondiente a una instalación radioeléctrica, se entenderá que ésta no está autorizada para su funcionamiento. La nueva puesta en servicio de esta instalación radioeléctrica deberá atenerse a lo establecido en los artículos 8 y 9 de este Reglamento.

2. En el plazo de un año, contando a partir de la entrada en vigor de este Reglamento, los operadores y titulares de licencias individuales a los que se refiere el apartado 1 del artículo 8, que dispongan de instalaciones radioeléctricas autorizadas con anterioridad a la fecha de entrada en vigor de este Reglamento, deberán tener adecuadas todas sus instalaciones radioeléctricas a lo previsto en el apartado 2 del artículo 8. Una vez concluida esta adecuación, lo comunicarán al Ministerio de Ciencia y Tecnología.

3. El Ministerio de Ciencia y Tecnología informará al Ministerio de Sanidad y Consumo sobre el grado de conformidad de las instalaciones radioeléctricas.

ANEXO I

Limitaciones y servidumbres para la protección de determinadas instalaciones radioeléctricas

(Derogado)

ANEXO II

Límites de exposición a las emisiones radioeléctricas

1. Definiciones

A) Magnitudes físicas: En el contexto de la exposición a las emisiones radioeléctricas, se emplean habitualmente las siguientes magnitudes físicas:

La corriente de contacto (Ic) entre una persona y un objeto se expresa en amperios (A). Un objeto conductor en un campo eléctrico puede ser cargado por el campo.

La densidad de corriente (J) se define como la corriente que fluye por una unidad de sección transversal perpendicular a la dirección de la corriente, en un conductor volumétrico, como puede ser el cuerpo humano o parte de éste, expresada en amperios por metro cuadrado (A/m^2).

La intensidad de campo eléctrico es una magnitud vectorial (E) que corresponde a la fuerza ejercida sobre una partícula cargada independientemente de su movimiento en el espacio. Se expresa en voltios por metro (V/m).

La intensidad de campo magnético es una magnitud vectorial (H) que, junto con la inducción magnética, determina un campo magnético en cualquier punto del espacio. Se expresa en amperios por metro (A/m).

La densidad de flujo magnético o inducción magnética es una magnitud vectorial (B) que da lugar a una fuerza que actúa sobre cargas en movimiento, y se expresa en teslas (T). En espacio libre y en materiales biológicos, la densidad de flujo o inducción magnética y la intensidad de campo magnético se pueden intercambiar utilizando la equivalencia 1 A/m = 4 π 10^{-7} T.

La densidad de potencia (S) es la magnitud utilizada para frecuencias muy altas, donde la profundidad de penetración en el cuerpo es baja. Es la potencia radiante que incide perpendicular a una superficie, dividida por el área de la superficie, y se expresa en vatios por metro cuadrado (W/m^2).

La absorción específica de energía (SA, «specific energy absorption») se define como la energía absorbida por unidad de masa de tejido biológico, expresada en julios por kilogramo (J/kg). En esta recomendación se utiliza para limitar los efectos no térmicos de la radiación de microondas pulsátil.

El índice de absorción específica de energía (SAR, «specific energy absorption rate»), se define como potencia absorbida por unidad de masa de tejido corporal, cuyo promedio se calcula en la totalidad del cuerpo o en partes de éste, y se expresa en vatios por kilogramo (W/kg). El SAR de cuerpo entero es una medida ampliamente aceptada para relacionar los efectos térmicos adversos con la exposición a las emisiones radioeléctricas. Junto al SAR medio de cuerpo entero, los valores SAR locales son necesarios para evaluar y limitar una deposición excesiva de energía en pequeñas partes del cuerpo como consecuencia de unas condiciones especiales de exposición. Ejemplos de tales condiciones son: La exposición a las emisiones radioeléctricas en la gama baja de Mhz de una persona en contacto con la tierra, o las personas expuestas en el espacio adyacente a una antena.

De entre estas magnitudes, las que pueden medirse directamente son la densidad de flujo magnético, la corriente de contacto, la intensidad del campo eléctrico y la del campo magnético y la densidad de potencia.

B) Restricciones básicas y niveles de referencia: Para la aplicación de las restricciones basadas en la evaluación de los posibles efectos de las emisiones radioeléctricas sobre la salud, se ha de diferenciar las restricciones básicas de los niveles de referencia.

Restricciones básicas. Las restricciones de la exposición a los campos eléctricos, magnéticos y electromagnéticos variables en el tiempo, basadas directamente en los efectos sobre la salud conocidos y en consideraciones biológicas, reciben el nombre de «restricciones básicas». Dependiendo de la frecuencia del campo, las magnitudes físicas empleadas para especificar estas restricciones son la inducción magnética (B), la densidad de corriente (J), el índice de absorción específica de energía (SAR) o la densidad de potencia (S). La inducción magnética y la densidad de potencia se pueden medir con facilidad en los individuos expuestos.

Niveles de referencia. Estos niveles se ofrecen a efectos prácticos de evaluación de la exposición, para determinar la probabilidad de que se sobrepasen las restricciones básicas. Algunos niveles de referencia se derivan de las restricciones básicas pertinentes utilizando mediciones o técnicas computerizadas, y algunos se refieren a la percepción y a los efectos adversos indirectos de la exposición a las emisiones radioeléctricas. Las magnitudes derivadas son la intensidad de campo eléctrico (E), la intensidad de campo magnético (H), la inducción magnética (B), la densidad de potencia (S) y la corriente en extremidades (I_l). Las magnitudes que se refieren a la percepción y otros efectos indirectos son la corriente (de contacto) (I_c) y, para los campos pulsátiles, la absorción específica de energía (SA). En cualquier situación particular de exposición, los valores medidos o calculados de cualquiera de estas cantidades pueden compararse con el nivel de referencia adecuado. El cumplimiento del nivel de referencia garantizará el respeto de la restricción básica pertinente. Que el valor medido sobrepase el nivel de referencia no quiere decir necesariamente que se

vaya a sobrepasar la restricción básica. Sin embargo, en tales circunstancias es necesario comprobar si ésta se respeta.

Algunas magnitudes, como la inducción magnética (B) y la densidad de potencia (S), sirven a determinadas frecuencias como restricciones básicas y como niveles de referencia.

Los límites de exposición a emisiones radioeléctricas a los que se refiere el Reglamento son los resultantes de aplicar las restricciones básicas y los niveles de referencia en zonas en las que pueda permanecer habitualmente el público en general, sin perjuicio de lo establecido en otras disposiciones específicas en el ámbito laboral.

2. Restricciones básicas

Dependiendo de la frecuencia, para especificar las restricciones básicas sobre los campos electromagnéticos se emplean las siguientes cantidades físicas (cantidades dosimétricas o exposimétricas):

a) Entre 0 y 1 Hz se proporcionan restricciones básicas de la inducción magnética para campos magnéticos estáticos (0 Hz) y de la densidad de corriente para campos variables en el tiempo de 1 Hz, con el fin de prevenir los efectos sobre el sistema cardiovascular y el sistema nervioso central.

b) Entre 1 Hz y 10 MHz se proporcionan restricciones básicas de la densidad de corriente para prevenir los efectos sobre las funciones del sistema nervioso.

c) Entre 100 kHz y 10 GHz se proporcionan restricciones básicas del SAR para prevenir la fatiga calorífica de cuerpo entero y un calentamiento local excesivo de los tejidos. En la gama de 100 kHz a 10 MHz se ofrecen restricciones de la densidad de corriente y del SAR.

d) Entre 10 GHz y 300 GHz se proporcionan restricciones básicas de la densidad de potencia, con el fin de prevenir el calentamiento de los tejidos en la superficie corporal o cerca de ella.

Las restricciones básicas expuestas en el cuadro 1 se han establecido teniendo en cuenta las variaciones que puedan introducir las sensibilidades individuales y las condiciones medioambientales, así como el hecho de que la edad y el estado de salud de los ciudadanos varían.

CUADRO 1

Restricciones básicas para campos eléctricos, magnéticos y electromagnéticos (0 Hz-300 GHz)

Gama de frecuencia	**Inducción magnética (mT)**	**Densidad de corriente (mA/m²) rms**	**SAR medio de cuerpo entero (W/kg)**	**SAR Localizado (cabeza y tronco) (W/kg)**	**SAR Localizado (miembros) (W/kg)**	**Densidad de potencia S (W/m²)**
0 Hz	40	–	–	–	–	–
>0-1 Hz	–	8	–	–	–	–
1-4 Hz-	–	8/f	–	–	–	–
4-1.000Hz	–	2	–	–	–	–
1.000 Hz-100 kHz	–	f/500	–	–	–	–
100 kHz-10 MHz	–	f/500	0,08	2	4	–
10 MHz-10 GHz	–	–	0,08	2	4	–
10-300 GHz	–	–	–	–	–	10

Notas:

1. f es la frecuencia en Hz.

2. El objetivo de la restricción básica de la densidad de corriente es proteger contra los graves efectos de la exposición sobre los tejidos del sistema nervioso central en la cabeza y en el tronco, e incluye un factor de seguridad. Las restricciones básicas para los campos frecuencias muy bajas se basan en los efectos negativos establecidos en el sistema nervioso central. Estos efectos agudos son esencialmente instantáneos y no existe justificación

científica para modificar las restricciones básicas en relación con las exposiciones de corta duración. Sin embargo, puesto que las restricciones básicas se refieren a los efectos negativos en el sistema nervioso central, estas restricciones básicas pueden permitir densidades más altas en los tejidos del cuerpo distintos de los del sistema nervioso central en iguales condiciones de exposición.

3. Dada la falta de homogeneidad eléctrica del cuerpo, debe calcularse el promedio de las densidades de corriente en una sección transversal de 1 cm^2 perpendicular a la dirección de la corriente.

4. Para frecuencias de hasta 100 kHz, los valores pico de densidad de corriente pueden obtenerse multiplicando el valor cuadrático medio (rms) por √2 (≈1,414). Para pulsos de duración t_p, la frecuencia equivalente que ha de aplicarse en las restricciones básicas debe calcularse como $f = 1/(2t_p)$.

5. Para frecuencias de hasta 100 kHz y para campos magnéticos pulsátiles, la densidad de corriente máxima asociada con los pulsos puede calcularse a partir de los tiempos de subida/caída y del índice máximo de cambio de la inducción magnética. La densidad de corriente inducida puede entonces compararse con la restricción básica correspondiente.

6. Todos los valores SAR deben ser promediados a lo largo de un período cualquiera de seis minutos.

7. La masa promediada de SAR localizado la constituye una porción cualquiera de 10 g de tejido contiguo; el SAR máximo obtenido de esta forma debe ser el valor que se utilice para evaluar la exposición. Estos 10 g de tejido se consideran como una masa de tejidos contiguos con propiedades eléctricas casi homogéneas. Especificando que se trata de una masa de tejidos contiguos, se reconoce que este concepto puede utilizarse en la dosimetría automatizada, aunque puede presentar dificultades a la hora de efectuar mediciones físicas directas. Puede utilizarse una geometría simple, como una masa de tejidos cúbica, siempre que las cantidades dosimétricas calculadas tengan valores de prudencia en relación con las directrices de exposición.

8. Para los pulsos de duración tp, la frecuencia equivalente que ha de aplicarse en las restricciones básicas debe calcularse como $f = 1/(2t_p)$. Además, en lo que se refiere a las exposiciones pulsátiles, en la gama de frecuencias de 0,3 a 10 GHz y en relación con la exposición localizada de la cabeza, la SA no debe sobrepasar los 2 mJ/kg^{-1} como promedio calculado en 10 g de tejido.

3. Niveles de referencia.

Los niveles de referencia de la exposición sirven para ser comparados con los valores de las magnitudes medidas. El respeto de todos los niveles de referencia asegurará el respeto de las restricciones básicas.

Si las cantidades de los valores medidos son mayores que los niveles de referencia, no significa necesariamente que se hayan sobrepasado las restricciones básicas. En este caso, debe efectuarse una evaluación para comprobar si los niveles de exposición son inferiores a las restricciones básicas.

Los niveles de referencia para limitar la exposición se obtienen a partir de las restricciones básicas, presuponiendo un acoplamiento máximo del campo con el individuo expuesto, con lo que se obtiene un máximo de protección. En los cuadros 2 y 3 figura un resumen de los niveles de referencia. Por lo general, éstos están pensados como valores promedio, calculados espacialmente sobre toda la extensión del cuerpo del individuo expuesto, pero teniendo muy en cuenta que no deben sobrepasarse las restricciones básicas de exposición localizadas.

En determinadas situaciones en las que la exposición está muy localizada, como ocurre con los teléfonos móviles y con la cabeza del individuo, no es apropiado emplear los niveles de referencia. En estos casos, debe evaluarse directamente si se respeta la restricción básica localizada.

3.1 Niveles de campo.

CUADRO 2

Niveles de referencia para campos eléctricos, magnéticos y electromagnéticos (0 Hz-300 GHz, valores rms imperturbados)

Gama de frecuencia	Intensidad de campo E – (V/m)	Intensidad de campo H – (A/m)	Campo B – (µT)	Densidad de potencia equivalente de onda plana – (W/m^2)
0-1 Hz	–	$3,2 \times 10^4$	4×10^4	
1-8 Hz	10.000	$3,2 \times 10^4/f^2$	$4 \times 10^4/f^2$	
8-25 Hz	10.000	4.000/f	5.000/f	
0,025-0,8 kHz	250/f	4/f	5/f	–
0,8-3 kHz	250/f	5	6,25	–
3-150 kHz	87	5	6,25	–
0,15-1 MHz	87	0,73/f	0,92/f	–
1-10 MHz	$87/f^{1/2}$	0,73/f	0,92/f	–
10-400 MHz	28	0,073	0,092	2
400-2.000 MHz	$1,375\ f^{1/2}$	$0,0037\ f^{1/2}$	$0,0046\ f^{1/2}$	f/200
2-300 GHz	61	0,16	0,20	10

Notas:

1. f según se indica en la columna de gama de frecuencia.

2. Para frecuencias de 100 kHz a 10 GHz, el promedio de S_{eq}, E^2, H^2 y B^2, ha de calcularse a lo largo de un período cualquiera de seis minutos.

3. Para frecuencias superiores a 10 GHz, el promedio de S_{eq}, E^2, H^2 y B^2, ha de calcularse a lo largo de un período cualquiera de $68/f^{1,05}$ minutos (f en GHz).

4. No se ofrece ningún valor de campo E para frecuencias <1 Hz. La mayor parte de las personas no percibirá las cargas eléctricas superficiales con resistencias de campo inferiores a 25 kV/m. En cualquier caso, deben evitarse las descargas de chispas, que causan estrés o molestias.

Nota: no se indican niveles de referencia más altos para la exposición a los campos de frecuencia extremadamente baja (FEB) cuando las exposiciones son de corta duración (véase nota 2 del cuadro 1). En muchos casos, cuando los valores medidos rebasan el nivel de referencia, no se deduce necesariamente que se haya rebasado la restricción básica. Siempre que puedan evitarse los impactos negativos para la salud de los efectos indirectos de la exposición (como los microshocks), se reconoce que pueden rebasarse los niveles de referencia, siempre que no se rebase la restricción básica relativa a la densidad de corriente.

En cuanto a valores de pico, se aplicarán los siguientes niveles de referencia para la intensidad de campo eléctrico (E) (V/m), la intensidad de campo magnético (H) (A/m) y a la inducción de campo magnético (B) (µT):

a) Para frecuencias de hasta 100 kHz, los valores de pico esta de referencia se obtienen multiplicando los valores rms correspondientes por √2 (≈1,414). Para pulsos de duración t_p, la frecuencia equivalente que ha de aplicarse debe calcularse como $f=1/(2t_p)$.

b) Para frecuencias de entre 100 kHz y 10 MHz, los valores de pico de referencia se obtienen multiplicando los valores rms correspondientes por 10^a, donde a = [0,665 log $(f/10^5)$ + 0,176], donde f se expresa en Hz.

c) Para frecuencias de entre 10 MHz y 300 GHz, los valores de referencia de pico se obtienen multiplicando los valores rms correspondientes por 32.

Nota: en lo que se refiere a frecuencias que sobrepasan los 10 MHz, el promedio Seq calculado en la anchura del pulso no debe ser mayor de 1.000 veces los niveles de referencia, o bien las intensidades de campo no deben ser mayores de 32 veces los niveles de referencia de intensidad de campo. Para frecuencias de entre unos 0,3 GHz y varios GHz, y en relación con la exposición localizada de la cabeza, debe limitarse la absorción específica derivada de los pulsos, para limitar o evitar los efectos auditivos causados por la extensión termoelástica. En esta gama de frecuencia, el umbral SA de 4-16 mJ/kg^{-1} que es

necesario para producir este efecto corresponde, para pulsos 30µS, a valores máximos SAR de 130 a 520 W/kg^{-1} en el cerebro. Entre 100 kHz y 10 MHz, los valores de pico de las intensidades de campo se obtienen mediante interpolación desde el pico multiplicado por 1,5 a 100 kHz hasta el pico multiplicado por 32 a 10 MHz.

3.2 Corrientes de contacto y corriente en extremidades: Para frecuencias de hasta 110 MHz se establecen niveles de referencia adicionales para evitar los peligros debidos a las corrientes de contacto. En el cuadro 3 figuran los niveles de referencia de corriente de contacto. Éstos se han establecido para tomar en consideración el hecho de que las corrientes de contacto umbral que provocan reacciones biológicas en mujeres adultas y niños, equivalen aproximadamente a dos tercios y la mitad, respectivamente, de las que corresponden a hombres adultos.

CUADRO 3

Niveles de referencia para corrientes de contacto procedentes de objetos conductores (f en kHz)

Gama de frecuencia	Corriente máxima de contacto (mA)
0 Hz-2,5 kHz	0,5
2,5 KHz-100 kHz	0,2 f
100 KHz-110 MHz	20

Para la gama de frecuencias de 10 MHz a 110 MHz, se establece un nivel de referencia 45 mA en términos de corriente a través de cualquier extremidad. Con ello, se pretende limitar el SAR localizado a lo largo de un período cualquiera de seis minutos.

4. Exposición a fuentes con múltiples frecuencias. En situaciones en las que se da una exposición simultánea a campos de diferentes frecuencias, debe tenerse en cuenta la posibilidad de que se sumen los efectos de estas exposiciones. Para cada efecto deben hacerse cálculos basados en esa actividad; así pues, deben efectuarse evaluaciones separadas de los efectos de la estimulación térmica y eléctrica sobre el cuerpo.

4.1 Restricciones básicas:

En el caso de la exposición simultánea a campos de diferentes frecuencias, deberán cumplirse los siguientes criterios como restricciones básicas.

En cuanto a la estimación eléctrica, pertinente en lo que se refiere a frecuencias de 1 Hz a 10 MHz, las densidades de corriente inducida deben cumplir lo siguiente:

$$\left. \sum_{i=1Hz}^{10MHz} \frac{J_i}{J_{L,i}} \leq 1 \right|$$

donde:

J_i es la densidad de corriente a la frecuencia i;

$J_{L,i}$ es la restricción básica de densidad de corriente a la frecuencia i, según figura en el cuadro1;

En lo que respecta a los efectos térmicos, pertinentes a partir de los 100 kHz, los índices de absorción específica de energía y las densidades de potencia deben cumplir lo siguiente:

$$\sum_{i=100kHz}^{10GHz} \frac{SAR_i}{SAR_L} + \sum_{i>10GHz}^{300GHz} \frac{S_i}{S_L} \leq 1$$

donde:

SAR_i es el SAR causado por la exposición a la frecuencia i;

SAR_L es la restricción básica de SAR que figura en el cuadro 1;

S_i es la densidad de potencia a la frecuencia i;

S_L es la restricción básica de densidad de potencia que figura en el cuadro 1.

4.2 Niveles de referencia:

1.º Para la aplicación práctica de las restricciones básicas deben considerarse los siguientes criterios relativos a los niveles de referencia de las intensidades de campo.

En relación con las densidades de corriente inducida y los efectos de estimulación eléctrica, pertinentes hasta los 10 MHz, a los niveles de campo deben aplicarse las dos exigencias siguientes:

$$\sum_{i=1Hz}^{1MHz} \frac{E_i}{E_{L,i}} + \sum_{i>1MHz}^{10MHz} \frac{E_i}{a} \leq 1$$

$$\sum_{j=1Hz}^{150kHz} \frac{H_j}{H_{L,j}} + \sum_{j>150kHz}^{10MHz} \frac{H_j}{b} \leq 1$$

donde:

E_i es la intensidad de campo eléctrico a la frecuencia i;
$E_{L,i}$ es el nivel de referencia de campo eléctrico del cuadro 2;
H_j es la densidad de campo magnético a la frecuencia j;
H_L,j es el nivel de referencia de campo magnético derivado del cuadro 2;
a es 87 V/m y b es 5 A/m (6,25 µT).

El uso de los valores constantes (a y b) por encima de 1 MHz en lo que respecta al campo eléctrico, y por encima de 150 kHz en lo que se refiere al campo magnético, se debe al hecho de que la suma está basada en densidades de corriente inducida y no debe mezclarse con las circunstancias de efectos térmicos. Esto último constituye la base para $E_{L,i}$ y $H_{L,j}$ por encima de 1 MHz y 150 kHz, respectivamente, que figuran en el cuadro 2.

En relación con las circunstancias de efecto térmico, pertinentes a partir de 100 kHz, a los niveles de campo deben aplicarse las dos exigencias siguientes:

$$\sum_{i=100kHz}^{1MHz}\left(\frac{E_i}{c}\right)^2+\sum_{i>1MHz}^{300GHz}\left(\frac{E_i}{E_{L,i}}\right)^2\leq 1$$

$$\sum_{j=100kHz}^{150kHz}\left(\frac{H_j}{d}\right)^2+\sum_{j>150kHz}^{300GHz}\left(\frac{H_j}{H_{L,j}}\right)^2\leq 1$$

donde:

E_j es la intensidad de campo eléctrico a la frecuencia i;
$E_{L,i}$ es el nivel de referencia de campo eléctrico del cuadro 2;
H_j es la densidad de campo magnético a la frecuencia j;
$H_{L,j}$ es el nivel de referencia de campo magnético derivado del cuadro 2;
c es 87/f1/2 V/m y d 0,73/f A/m, donde f es la frecuencia expresada en MHz.

2.º Para la corriente de extremidades y la corriente de contacto, respectivamente, deben aplicarse las siguientes exigencias:

$$\sum_{k=10MHz}^{110MHz}\left(\frac{I_k}{I_{L,k}}\right)^2 \leq 1; \sum_{n\rangle 1Hz}^{110MHz}\left(\frac{I_n}{I_{C,n}}\right)^2 \leq 1$$

donde:

I_k es el componente de corriente de extremidades a la frecuencia k;

$I_{L,k}$ es el nivel de referencia de la corriente de extremidades, 45 mA;

I_n es el componente de corriente de contacto a la frecuencia n;

$I_{C,n}$ es el nivel de referencia de la corriente de contacto a la frecuencia n (véase el cuadro 3);

Las anteriores fórmulas de adición presuponen las peores condiciones de fase entre los campos. En consecuencia, las situaciones típicas de exposición pueden dar lugar, en la práctica, a unos niveles de exposición menos restrictivos de lo que indican las fórmulas correspondientes a los niveles de referencia.

5. Métodos de medida y referencias.

En lo relativo a los métodos de medidas, tipos de instrumentación y otros requisitos se estará a lo recogido en las normas técnicas aplicables, con el orden de prelación que figura en el artículo 11.

§ 43

Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones

Jefatura del Estado
«BOE» núm. 251, de 19 de octubre de 2007
Última modificación: 10 de mayo de 2014
Referencia: BOE-A-2007-18243

JUAN CARLOS I

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley.

PREÁMBULO

I

La aplicación de las nuevas tecnologías desarrolladas en el marco de la sociedad de la información ha supuesto la superación de las formas tradicionales de comunicación, mediante una expansión de los contenidos transmitidos, que abarcan no sólo la voz, sino también datos en soportes y formatos diversos. A su vez, esta extraordinaria expansión en cantidad y calidad ha venido acompañada de un descenso en los costes, haciendo que este tipo de comunicaciones se encuentre al alcance de cualquier persona y en cualquier rincón del mundo.

La naturaleza neutra de los avances tecnológicos en telefonía y comunicaciones electrónicas no impide que su uso pueda derivarse hacia la consecución de fines indeseados, cuando no delictivos.

Precisamente en el marco de este último objetivo se encuadra la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, y por la que se modifica la Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio, cuya transposición a nuestro ordenamiento jurídico es el objetivo principal de esta Ley.

El objeto de esta Directiva es establecer la obligación de los operadores de telecomunicaciones de retener determinados datos generados o tratados por los mismos, con el fin de posibilitar que dispongan de ellos los agentes facultados. Se entienden por agentes facultados los miembros de los Cuerpos Policiales autorizados para ello en el marco de una investigación criminal por la comisión de un delito, el personal del Centro Nacional de

Inteligencia para llevar a cabo una investigación de seguridad amparada en la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, y en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia, así como los funcionarios de la Dirección Adjunta de Vigilancia Aduanera, en el desarrollo de sus competencias como policía judicial, de acuerdo con el apartado 1 del artículo 283 de la Ley de Enjuiciamiento Criminal. Se trata, pues, de que todos éstos puedan obtener los datos relativos a las comunicaciones que, relacionadas con una investigación, se hayan podido efectuar por medio de la telefonía fija o móvil, así como por Internet. El establecimiento de esas obligaciones, justificado en aras de proteger la seguridad pública, se ha efectuado buscando el imprescindible equilibrio con el respeto de los derechos individuales que puedan verse afectados, como son los relativos a la privacidad y la intimidad de las comunicaciones.

En este sentido, la Ley es respetuosa con los pronunciamientos que, en relación con el derecho al secreto de las comunicaciones, ha venido emitiendo el Tribunal Constitucional, respeto que, especialmente, se articula a través de dos garantías: en primer lugar, que los datos sobre los que se establece la obligación de conservación son datos exclusivamente vinculados a la comunicación, ya sea telefónica o efectuada a través de Internet, pero en ningún caso reveladores del contenido de ésta; y, en segundo lugar, que la cesión de tales datos que afecten a una comunicación o comunicaciones concretas, exigirá, siempre, la autorización judicial previa.

En relación con esta última precisión, cabe señalar que la Directiva se refiere, expresamente, a que los datos conservados deberán estar disponibles a los fines de detección o investigación por delitos graves, definidos éstos de acuerdo con la legislación interna de cada Estado miembro.

II

La Ley cuenta con diez artículos que se agrupan en tres capítulos.

El Capítulo I («Disposiciones Generales») se inicia describiendo su objeto, que básicamente se circunscribe a la determinación de la obligación de conservar los datos enumerados en el artículo 3, que se hayan generado o tratado en el marco de una comunicación de telefonía fija o móvil, o realizada a través de una comunicación electrónica de acceso público o mediante una red pública de comunicaciones. Igualmente, se precisan los fines que, exclusivamente, justifican la obligación de conservación, y que se limitan a la detección, investigación y enjuiciamiento de un delito contemplado en el Código Penal o las leyes penales especiales, con los requisitos y cautelas que la propia Ley establece.

En este capítulo también se precisan las limitaciones sobre el tipo de datos a retener, que son los necesarios para identificar el origen y destino de la comunicación, así como la identidad de los usuarios o abonados de ambos, pero nunca datos que revelen el contenido de la comunicación. Igualmente, la Ley impone la obligación de conservación de datos que permitan determinar el momento y duración de una determinada comunicación, su tipo, así como datos necesarios para identificar el equipo de comunicación empleado y, en el caso de utilización de un equipo móvil, los datos necesarios para su localización.

En relación con los sujetos que quedan obligados a conservar los datos, éstos serán los operadores que presten servicios de comunicaciones electrónicas disponibles al público, o que exploten una red pública de comunicaciones electrónicas en España.

La Ley enumera en su artículo 3, de manera precisa y detallada, el listado de datos que quedan sujetos a la obligación de conservación en el marco de las comunicaciones por telefonía fija, móvil o Internet. Estos datos, que, se repite, en ningún caso revelarán el contenido de la comunicación, son los necesarios para identificar el origen y destino de la comunicación, su hora, fecha y duración, el tipo de servicio utilizado y el equipo de comunicación de los usuarios utilizado. En aplicación de las previsiones contenidas en la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo, quedan incluidas también en el ámbito de aplicación de la Ley las denominadas llamadas telefónicas infructuosas. Igualmente se incluye la obligación de conservar los elementos que sean suficientes para identificar el momento de activación de los teléfonos que funcionen bajo la modalidad de prepago.

En el Capítulo II («Conservación y cesión de datos») se establecen los límites para efectuar la cesión de datos, el plazo de conservación de los mismos, que será, con carácter

general, de doce meses desde que la comunicación se hubiera establecido (si bien reglamentariamente se podrá reducir a seis meses o ampliar a dos años, como permite la Directiva 2006/24/CE), y los instrumentos para garantizar el uso legítimo de los datos conservados, cuya cesión y entrega exclusivamente se podrá efectuar al agente facultado y para los fines establecidos en la Ley, estando cualquier uso indebido sometido a los mecanismos de control de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo. Además, se establecen previsiones específicas respecto al régimen general regulador de los derechos de acceso, rectificación y cancelación de datos contenido en la referida Ley Orgánica 15/1999.

El Capítulo III, al referirse al régimen sancionador, remite, en cuanto a los incumplimientos de las obligaciones de conservación y protección y seguridad de los datos de carácter personal, a la regulación contenida en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones. Por otro lado, los incumplimientos de la obligación de puesta a disposición de los agentes facultados, en la medida en que las solicitudes estarán siempre amparadas por orden judicial, constituirían la correspondiente infracción penal.

En las disposiciones contenidas en la parte final se incluyen contenidos diversos. Por un lado, y a los efectos de poder establecer instrumentos para controlar el empleo para fines delictivos de los equipos de telefonía móvil adquiridos mediante la modalidad de prepago, se establece, como obligación de los operadores que comercialicen dicho servicio, la llevanza de un registro con la identidad de los compradores.

Por último, la Ley incorpora en las disposiciones finales una modificación de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, para adaptarla al contenido de esta Ley, una referencia a su amparo competencial, una habilitación general al Gobierno para su desarrollo y un período de seis meses para que las operadoras puedan adaptarse a su contenido.

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto de la Ley.*

1. Esta Ley tiene por objeto la regulación de la obligación de los operadores de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación, así como el deber de cesión de dichos datos a los agentes facultados siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales.

2. Esta Ley se aplicará a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o usuario registrado.

3. Se excluye del ámbito de aplicación de esta Ley el contenido de las comunicaciones electrónicas, incluida la información consultada utilizando una red de comunicaciones electrónicas.

Artículo 2. *Sujetos obligados.*

Son destinatarios de las obligaciones relativas a la conservación de datos impuestas en esta Ley los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones, en los términos establecidos en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

Artículo 3. *Datos objeto de conservación.*

1. Los datos que deben conservarse por los operadores especificados en el artículo 2 de esta Ley, son los siguientes:

a) Datos necesarios para rastrear e identificar el origen de una comunicación:

1.° Con respecto a la telefonía de red fija y a la telefonía móvil:

i) Número de teléfono de llamada.
ii) Nombre y dirección del abonado o usuario registrado.

2.° Con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet:

i) La identificación de usuario asignada.
ii) La identificación de usuario y el número de teléfono asignados a toda comunicación que acceda a la red pública de telefonía.
iii) El nombre y dirección del abonado o del usuario registrado al que se le ha asignado en el momento de la comunicación una dirección de Protocolo de Internet (IP), una identificación de usuario o un número de teléfono.

b) Datos necesarios para identificar el destino de una comunicación:

1.º Con respecto a la telefonía de red fija y a la telefonía móvil:

i) El número o números marcados (el número o números de teléfono de destino) y, en aquellos casos en que intervengan otros servicios, como el desvío o la transferencia de llamadas, el número o números hacia los que se transfieren las llamadas.
ii) Los nombres y las direcciones de los abonados o usuarios registrados.

2.º Con respecto al correo electrónico por Internet y la telefonía por Internet:

i) La identificación de usuario o el número de teléfono del destinatario o de los destinatarios de una llamada telefónica por Internet.
ii) Los nombres y direcciones de los abonados o usuarios registrados y la identificación de usuario del destinatario de la comunicación.

c) Datos necesarios para determinar la fecha, hora y duración de una comunicación:

1.° Con respecto a la telefonía de red fija y a la telefonía móvil: la fecha y hora del comienzo y fin de la llamada o, en su caso, del servicio de mensajería o del servicio multimedia.
2.° Con respecto al acceso a Internet, al correo electrónico por Internet y a la telefonía por Internet:

i) La fecha y hora de la conexión y desconexión del servicio de acceso a Internet registradas, basadas en un determinado huso horario, así como la dirección del Protocolo Internet, ya sea dinámica o estática, asignada por el proveedor de acceso a Internet a una comunicación, y la identificación de usuario o del abonado o del usuario registrado.
ii) La fecha y hora de la conexión y desconexión del servicio de correo electrónico por Internet o del servicio de telefonía por Internet, basadas en un determinado huso horario.

d) Datos necesarios para identificar el tipo de comunicación.

1.° Con respecto a la telefonía de red fija y a la telefonía móvil: el servicio telefónico utilizado: tipo de llamada (transmisión de voz, buzón vocal, conferencia, datos), servicios suplementarios (incluido el reenvío o transferencia de llamadas) o servicios de mensajería o multimedia empleados (incluidos los servicios de mensajes cortos, servicios multimedia avanzados y servicios multimedia).
2.° Con respecto al correo electrónico por Internet y a la telefonía por Internet: el servicio de Internet utilizado.

e) Datos necesarios para identificar el equipo de comunicación de los usuarios o lo que se considera ser el equipo de comunicación:

1.º Con respecto a la telefonía de red fija: los números de teléfono de origen y de destino.
2.° Con respecto a la telefonía móvil:

i) Los números de teléfono de origen y destino.
ii) La identidad internacional del abonado móvil (IMSI) de la parte que efectúa la llamada.
iii) La identidad internacional del equipo móvil (IMEI) de la parte que efectúa la llamada.
iv) La IMSI de la parte que recibe la llamada.

v) La IMEI de la parte que recibe la llamada.

vi) En el caso de los servicios anónimos de pago por adelantado, tales como los servicios con tarjetas prepago, fecha y hora de la primera activación del servicio y la etiqueta de localización (el identificador de celda) desde la que se haya activado el servicio.

3.° Con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet:

i) El número de teléfono de origen en caso de acceso mediante marcado de números.

ii) La línea digital de abonado (DSL) u otro punto terminal identificador del autor de la comunicación.

f) Datos necesarios para identificar la localización del equipo de comunicación móvil:

1.° La etiqueta de localización (identificador de celda) al inicio de la comunicación.

2.° Los datos que permiten fijar la localización geográfica de la celda, mediante referencia a la etiqueta de localización, durante el período en el que se conservan los datos de las comunicaciones.

2. Ningún dato que revele el contenido de la comunicación podrá conservarse en virtud de esta Ley.

CAPÍTULO II

Conservación y cesión de datos

Artículo 4. *Obligación de conservar datos.*

1. Los sujetos obligados adoptarán las medidas necesarias para garantizar que los datos especificados en el artículo 3 de esta Ley se conserven de conformidad con lo dispuesto en ella, en la medida en que sean generados o tratados por aquéllos en el marco de la prestación de los servicios de comunicaciones de que se trate.

En ningún caso, los sujetos obligados podrán aprovechar o utilizar los registros generados, fuera de los supuestos de autorización fijados en el artículo 38 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

2. La citada obligación de conservación se extiende a los datos relativos a las llamadas infructuosas, en la medida que los datos son generados o tratados y conservados o registrados por los sujetos obligados. Se entenderá por llamada infructuosa aquella comunicación en el transcurso de la cual se ha realizado con éxito una llamada telefónica pero sin contestación, o en la que ha habido una intervención por parte del operador u operadores involucrados en la llamada.

3. Los datos relativos a las llamadas no conectadas están excluidos de las obligaciones de conservación contenidas en esta Ley. Se entenderá por llamada no conectada aquella comunicación en el transcurso de la cual se ha realizado sin éxito una llamada telefónica, sin que haya habido intervención del operador u operadores involucrados.

Artículo 5. *Período de conservación de los datos.*

1. La obligación de conservación de datos impuesta cesa a los doce meses computados desde la fecha en que se haya producido la comunicación. Reglamentariamente, previa consulta a los operadores, se podrá ampliar o reducir el plazo de conservación para determinados datos o una categoría de datos hasta un máximo de dos años o un mínimo de seis meses, tomando en consideración el coste del almacenamiento y conservación de los datos, así como el interés de los mismos para los fines de investigación, detección y enjuiciamiento de un delito grave, previa consulta a los operadores.

2. Lo dispuesto en el apartado anterior se entiende sin perjuicio de lo previsto en el artículo 16.3 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, sobre la obligación de conservar datos bloqueados en los supuestos legales de cancelación.

Artículo 6. *Normas generales sobre cesión de datos.*

1. Los datos conservados de conformidad con lo dispuesto en esta Ley sólo podrán ser cedidos de acuerdo con lo dispuesto en ella para los fines que se determinan y previa autorización judicial.

2. La cesión de la información se efectuará mediante formato electrónico únicamente a los agentes facultados, y deberá limitarse a la información que resulte imprescindible para la consecución de los fines señalados en el artículo 1.

A estos efectos, tendrán la consideración de agentes facultados:

a) Los miembros de las Fuerzas y Cuerpos de Seguridad, cuando desempeñen funciones de policía judicial, de acuerdo con lo previsto en el artículo 547 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

b) Los funcionarios de la Dirección Adjunta de Vigilancia Aduanera, en el desarrollo de sus competencias como policía judicial, de acuerdo con el apartado 1 del artículo 283 de la Ley de Enjuiciamiento Criminal.

c) El personal del Centro Nacional de Inteligencia en el curso de las investigaciones de seguridad sobre personas o entidades, de acuerdo con lo previsto en la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, y en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia.

Artículo 7. *Procedimiento de cesión de datos.*

1. Los operadores estarán obligados a ceder al agente facultado los datos conservados a los que se refiere el artículo 3 de esta Ley concernientes a comunicaciones que identifiquen a personas, sin perjuicio de la resolución judicial prevista en el apartado siguiente.

2. La resolución judicial determinará, conforme a lo previsto en la Ley de Enjuiciamiento Criminal y de acuerdo con los principios de necesidad y proporcionalidad, los datos conservados que han de ser cedidos a los agentes facultados.

3. El plazo de ejecución de la orden de cesión será el fijado por la resolución judicial, atendiendo a la urgencia de la cesión y a los efectos de la investigación de que se trate, así como a la naturaleza y complejidad técnica de la operación.

Si no se establece otro plazo distinto, la cesión deberá efectuarse dentro del plazo de 7 días naturales contados a partir de las 8:00 horas del día natural siguiente a aquél en que el sujeto obligado reciba la orden.

Artículo 8. *Protección y seguridad de los datos.*

1. Los sujetos obligados deberán identificar al personal especialmente autorizado para acceder a los datos objeto de esta Ley, adoptar las medidas técnicas y organizativas que impidan su manipulación o uso para fines distintos de los comprendidos en la misma, su destrucción accidental o ilícita y su pérdida accidental, así como su almacenamiento, tratamiento, divulgación o acceso no autorizados, con sujeción a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y en su normativa de desarrollo.

2. Las obligaciones relativas a las medidas para garantizar la calidad de los datos y la confidencialidad y seguridad en el tratamiento de los mismos serán las establecidas en la Ley Orgánica 15/1999, de 13 de diciembre, y su normativa de desarrollo.

3. El nivel de protección de los datos almacenados se determinará de conformidad con lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, y en su normativa de desarrollo.

4. La Agencia Española de Protección de Datos es la autoridad pública responsable de velar por el cumplimiento de las previsiones de la Ley Orgánica 15/1999, de 13 de diciembre, y de la normativa de desarrollo aplicables a los datos contemplados en la presente Ley.

Artículo 9. *Excepciones a los derechos de acceso y cancelación.*

1. El responsable del tratamiento de los datos no comunicará la cesión de datos efectuada de conformidad con esta Ley.

2. El responsable del tratamiento de los datos denegará el ejercicio del derecho de cancelación en los términos y condiciones previstos en la Ley Orgánica 15/1999, de 13 de diciembre.

CAPÍTULO III

Infracciones y sanciones

Artículo 10. *Infracciones y sanciones.*

1. Constituyen infracciones a lo previsto en la presente Ley las siguientes:

a) Es infracción muy grave la no conservación en ningún momento de los datos a los que se refiere el artículo 3.

b) Son infracciones graves:

i) La no conservación reiterada o sistemática de los datos a los que se refiere el artículo 3.

ii) La conservación de los datos por un período inferior al establecido en el artículo 5.

iii) El incumplimiento deliberado de las obligaciones de protección y seguridad de los datos establecidas en el artículo 8.

c) Son infracciones leves:

i) La no conservación de los datos a los que se refiere el artículo 3 cuando no se califique como infracción muy grave o grave.

ii) El incumplimiento de las obligaciones de protección y seguridad de los datos establecidas en el artículo 8, cuando no se califique como infracción grave.

2. A las infracciones previstas en el apartado anterior, a excepción de las indicadas en los apartados 1.b).iii y 1.c).ii de este artículo, les será de aplicación el régimen sancionador establecido en la Ley General de Telecomunicaciones, correspondiendo la competencia sancionadora al Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información, sin perjuicio de las responsabilidades penales que pudieran derivar del incumplimiento de la obligación de cesión de datos a los agentes facultados.

El procedimiento para sancionar las citadas infracciones se iniciará por acuerdo del Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información, pudiendo el Ministerio del Interior instar dicho inicio.

En todo caso, se deberá recabar del Ministerio del Interior informe preceptivo y determinante para la resolución del procedimiento sancionador.

3. A las infracciones previstas en los apartados 1.b).iii y 1.c).ii de este artículo les será de aplicación el régimen sancionador establecido en la Ley General de Telecomunicaciones, correspondiendo la competencia sancionadora a la Agencia Española de Protección de Datos.

Disposición adicional única. *Servicios de telefonía mediante tarjetas de prepago.*

1. Los operadores de servicios de telefonía móvil que comercialicen servicios con sistema de activación mediante la modalidad de tarjetas de prepago, deberán llevar un libro-registro en el que conste la identidad de los clientes que adquieran una tarjeta inteligente con dicha modalidad de pago.

Los operadores informarán a los clientes, con carácter previo a la venta, de la existencia y contenido del registro, de su disponibilidad en los términos expresados en el número siguiente y de los derechos recogidos en el artículo 38.6 de la Ley 32/2003.

La identificación se efectuará mediante documento acreditativo de la personalidad, haciéndose constar en el libro-registro el nombre, apellidos y nacionalidad del comprador, así como el número correspondiente al documento identificativo utilizado y la naturaleza o denominación de dicho documento. En el supuesto de personas jurídicas, la identificación se realizará aportando la tarjeta de identificación fiscal, y se hará constar en el libro-registro la denominación social y el código de identificación fiscal.

2. Desde la activación de la tarjeta de prepago y hasta que cese la obligación de conservación a que se refiere el artículo 5 de esta Ley, los operadores cederán los datos identificativos previstos en el apartado anterior, cuando para el cumplimiento de sus fines les sean requeridos por los agentes facultados, los miembros de las Fuerzas y Cuerpos de Seguridad del Estado y de los Cuerpos Policiales de las Comunidades Autónomas con competencia para la protección de las personas y bienes y para el mantenimiento de la

seguridad pública, el personal del Centro Nacional de Inteligencia en el curso de las investigaciones de seguridad sobre personas o entidades, así como los funcionarios de la Dirección Adjunta de Vigilancia Aduanera.

3. Los datos identificativos estarán sometidos a las disposiciones de esta Ley, respecto a los sistemas que garanticen su conservación, no manipulación o acceso ilícito, destrucción, cancelación e identificación de la persona autorizada.

4. Los operadores deberán ceder los datos identificativos previstos en el apartado 1 de esta disposición a los agentes facultados, a los miembros de las Fuerzas y Cuerpos de Seguridad del Estado y de los Cuerpos Policiales de las Comunidades Autónomas con competencia para la protección de las personas y bienes y para el mantenimiento de la seguridad pública, o al personal del Centro Nacional de Inteligencia, así como a los funcionarios de la Dirección Adjunta de Vigilancia Aduanera, cuando les sean requeridos por éstos con fines de investigación, detección y enjuiciamiento de un delito contemplado en el Código Penal o en las leyes penales especiales.

5. Constituyen infracciones a lo previsto en la presente disposición, además de la previstas en el artículo 10, las siguientes:

a) Es infracción muy grave el incumplimiento de la llevanza del libro-registro referido.

b) Son infracciones graves la llevanza reiterada o sistemáticamente incompleta de dicho libro-registro así como el incumplimiento deliberado de la cesión y entrega de los datos a las personas y en los casos previstos en esta disposición.

c) Son infracciones leves la llevanza incompleta del libro-registro o el incumplimiento de la cesión y entrega de los datos a las personas y en los casos previstos en esta disposición cuando no se califiquen como infracciones muy graves o graves.

6. A las infracciones previstas en el apartado anterior les será de aplicación el régimen sancionador establecido en la Ley 32/2003, de 3 de noviembre, correspondiendo la competencia sancionadora al Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información.

El procedimiento para sancionar las citadas infracciones se iniciará por acuerdo del Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información, pudiendo el Ministerio del Interior instar dicho inicio.

En todo caso, se deberá recabar del Ministerio del Interior informe preceptivo y determinante para la resolución del procedimiento sancionador.

7. La obligación de inscripción en el libro-registro de los datos identificativos de los compradores que adquieran tarjetas inteligentes, así como el resto de obligaciones contenidas en la presente disposición adicional, comenzarán a ser exigibles a partir de la entrada en vigor de esta Ley.

8. No obstante, por lo que se refiere a las tarjetas adquiridas con anterioridad a la entrada en vigor de esta Ley, los operadores de telefonía móvil que comercialicen estos servicios dispondrán de un plazo de dos años, a contar desde dicha entrada en vigor, para cumplir con las obligaciones de inscripción a que se refiere el apartado 1 de la presente disposición adicional.

Transcurrido el aludido plazo de dos años, los operadores vendrán obligados a anular o a desactivar aquellas tarjetas de prepago respecto de las que no se haya podido cumplir con las obligaciones de inscripción del referido apartado 1 de esta disposición adicional, sin perjuicio de la compensación que, en su caso, corresponda al titular de las mismas por el saldo pendiente de consumo.

Disposición transitoria única. *Vigencia del régimen de interceptación de telecomunicaciones.*

Las normas dictadas en desarrollo del Capítulo III del Título III de la Ley 32/2003, de 3 de noviembre, continuarán en vigor en tanto no se opongan a lo dispuesto en esta Ley.

Disposición derogatoria única. *Derogación normativa.*

1. Quedan derogados los artículos 12, 38.2 c) y d) y 38.3 a) de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.

2. Asimismo, quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en esta Ley.

Disposición final primera. *Modificación de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.*

La Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, se modifica en los siguientes términos:

Uno. El artículo 33 queda redactado de la siguiente forma:

«Artículo 33. *Secreto de las comunicaciones.*

1. Los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público deberán garantizar el secreto de las comunicaciones de conformidad con los artículos 18.3 y 55.2 de la Constitución, debiendo adoptar las medidas técnicas necesarias.

2. Los operadores están obligados a realizar las interceptaciones que se autoricen de acuerdo con lo establecido en el artículo 579 de la Ley de Enjuiciamiento Criminal, en la Ley Orgánica 2/2002, de 6 de mayo, Reguladora del Control Judicial Previo del Centro Nacional de Inteligencia y en otras normas con rango de ley orgánica. Asimismo, deberán adoptar a su costa las medidas que se establecen en este artículo y en los reglamentos correspondientes.

3. La interceptación a que se refiere el apartado anterior deberá facilitarse para cualquier comunicación que tenga como origen o destino el punto de terminación de red o el terminal específico que se determine a partir de la orden de interceptación legal, incluso aunque esté destinada a dispositivo de almacenamiento o procesamiento de la información; asimismo, la interceptación podrá realizarse sobre un terminal conocido y con unos datos de ubicación temporal para comunicaciones desde locales públicos. Cuando no exista una vinculación fija entre el sujeto de la interceptación y el terminal utilizado, este podrá ser determinado dinámicamente cuando el sujeto de la interceptación lo active para la comunicación mediante un código de identificación personal.

4. El acceso se facilitará para todo tipo de comunicaciones electrónicas, en particular, por su penetración y cobertura, para las que se realicen mediante cualquier modalidad de los servicios de telefonía y de transmisión de datos, se trate de comunicaciones de vídeo, audio, intercambio de mensajes, ficheros o de la transmisión de facsímiles.

El acceso facilitado servirá tanto para la supervisión como para la transmisión a los centros de recepción de las interceptaciones de la comunicación electrónica interceptada y la información relativa a la interceptación, y permitirá obtener la señal con la que se realiza la comunicación.

5. Los sujetos obligados deberán facilitar al agente facultado, salvo que por las características del servicio no estén a su disposición y sin perjuicio de otros datos que puedan ser establecidos mediante real decreto, los datos indicados en la orden de interceptación legal, de entre los que se relacionan a continuación:

a) Identidad o identidades del sujeto objeto de la medida de la interceptación.

Se entiende por identidad: etiqueta técnica que puede representar el origen o el destino de cualquier tráfico de comunicaciones electrónicas, en general identificada mediante un número de identidad de comunicaciones electrónicas físico (tal como un número de teléfono) o un código de identidad de comunicaciones electrónicas lógico o virtual (tal como un número personal) que el abonado puede asignar a un acceso físico caso a caso.

b) Identidad o identidades de las otras partes involucradas en la comunicación electrónica.

c) Servicios básicos utilizados.

d) Servicios suplementarios utilizados.

e) Dirección de la comunicación.

f) Indicación de respuesta.

g) Causa de finalización.
h) Marcas temporales.
i) Información de localización.
j) Información intercambiada a través del canal de control o señalización.

6. Además de la información relativa a la interceptación prevista en el apartado anterior, los sujetos obligados deberán facilitar al agente facultado, salvo que por las características del servicio no estén a su disposición y sin perjuicio de otros datos que puedan ser establecidos mediante real decreto, de cualquiera de las partes que intervengan en la comunicación que sean clientes del sujeto obligado, los siguientes datos:

a) Identificación de la persona física o jurídica.
b) Domicilio en el que el proveedor realiza las notificaciones.
Y, aunque no sea abonado, si el servicio de que se trata permite disponer de alguno de los siguientes:
c) Número de titular de servicio (tanto el número de directorio como todas las identificaciones de comunicaciones electrónicas del abonado).
d) Número de identificación del terminal.
e) Número de cuenta asignada por el proveedor de servicios Internet.
f) Dirección de correo electrónico.

7. Junto con los datos previstos en los apartados anteriores, los sujetos obligados deberán facilitar, salvo que por las características del servicio no esté a su disposición, información de la situación geográfica del terminal o punto de terminación de red origen de la llamada, y de la del destino de la llamada. En caso de servicios móviles, se proporcionará una posición lo más exacta posible del punto de comunicación y, en todo caso, la identificación, localización y tipo de la estación base afectada.
8. Con carácter previo a la ejecución de la orden de interceptación legal, los sujetos obligados deberán facilitar al agente facultado información sobre los servicios y características del sistema de telecomunicación que utilizan los sujetos objeto de la medida de la interceptación y, si obran en su poder, los correspondientes nombres de los abonados con sus números de documento nacional de identidad, tarjeta de residencia o pasaporte, en el caso de personas físicas, o denominación y código de identificación fiscal en el caso de personas jurídicas.
9. Los sujetos obligados deberán tener en todo momento preparadas una o más interfaces a través de las cuales las comunicaciones electrónicas interceptadas y la información relativa a la interceptación se transmitirán a los centros de recepción de las interceptaciones. Las características de estas interfaces y el formato para la transmisión de las comunicaciones interceptadas a estos centros estarán sujetas a las especificaciones técnicas que reglamentariamente se establezcan por el Ministerio de Industria, Turismo y Comercio.
10. En el caso de que los sujetos obligados apliquen a las comunicaciones objeto de interceptación legal algún procedimiento de compresión, cifrado, digitalización o cualquier otro tipo de codificación, deberán entregar aquellas desprovistas de los efectos de tales procedimientos, siempre que sean reversibles.
Las comunicaciones interceptadas deben proveerse al centro de recepción de las interceptaciones con una calidad no inferior a la que obtiene el destinatario de la comunicación.»

Dos. El último párrafo del apartado 5 del artículo 38 pasa a tener la siguiente redacción:

«Lo establecido en las letras a) y d) del apartado 3 de este artículo se entiende sin perjuicio de las obligaciones establecidas en la Ley de Conservación de Datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones.»

Tres. En el artículo 53, se modifican los párrafos o) y z), que quedan redactados de la siguiente forma:

«o) El incumplimiento deliberado, por parte de los operadores, de las obligaciones en materia de interceptación legal de comunicaciones impuestas en desarrollo del artículo 33 de esta Ley y el incumplimiento deliberado de las obligaciones de conservación de los datos establecidas en la Ley de Conservación de Datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones.»

«z) La vulneración grave o reiterada de los derechos previstos en el artículo 38.3, salvo el previsto por el párrafo h), cuya infracción se regirá por el régimen sancionador previsto en la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, y el incumplimiento grave o reiterado de las obligaciones de protección y seguridad de los datos almacenados establecidas en el artículo 8 de la Ley de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.»

Cuatro. En el artículo 54 se modifican los párrafos ñ) y r), que quedan redactados de la siguiente forma:

«ñ) El incumplimiento, por parte de los operadores, de las obligaciones en materia de interceptación legal de comunicaciones impuestas en desarrollo del artículo 33 de la presente Ley y el incumplimiento de las obligaciones de conservación de los datos establecidas en la Ley de Conservación de Datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones, salvo que deban considerarse como infracción muy grave, conforme a lo dispuesto en el artículo anterior.»

«r) La vulneración de los derechos previstos en el artículo 38.3, salvo el previsto por el párrafo h), cuya infracción se regirá por el régimen sancionador previsto en la Ley 34/2002, de 11 de julio, y el incumplimiento de las obligaciones de protección y seguridad de los datos establecidas en el artículo 8 de la Ley de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, salvo que deban considerarse como infracción muy grave.»

Disposición final segunda. *Competencia estatal.*

Esta Ley se dicta al amparo de lo dispuesto en el artículo 149.1.29.ª de la Constitución, que atribuye al Estado la competencia exclusiva en materia de seguridad pública, y del artículo 149.1.21.ª, que confiere al Estado competencia exclusiva en materia de telecomunicaciones.

Disposición final tercera. *Desarrollo reglamentario.*

Se habilita al Gobierno a dictar cuantas disposiciones sean necesarias para el desarrollo y ejecución de lo previsto en esta Ley.

Disposición final cuarta. *Formato de entrega de los datos.*

1. La cesión a los agentes facultados de los datos cuya conservación sea obligatoria, se efectuará en formato electrónico, en la forma que se determine por Orden conjunta de los Ministros de Interior, de Defensa y de Economía y Hacienda, que se aprobará en el plazo de tres meses desde la entrada en vigor de esta Ley.

2. Los sujetos obligados a los que se refiere el artículo 2 de esta Ley, tendrán un plazo de seis meses desde la entrada en vigor de la misma para configurar, a su costa, sus equipos y estar técnicamente en disposición de cumplir con las obligaciones de conservación y cesión de datos.

Disposición final quinta. *Entrada en vigor.*

Esta Ley entrará en vigor a los veinte días de su publicación en el «Boletín Oficial del Estado».

§ 44

Orden PRE/199/2013, de 29 de enero, por la que se define el formato de entrega de los datos conservados por los operadores de servicios de comunicaciones electrónicas o de redes públicas de comunicaciones a los agentes facultados

Ministerio de la Presidencia
«BOE» núm. 40, de 15 de febrero de 2013
Última modificación: sin modificaciones
Referencia: BOE-A-2013-1591

La Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, tiene por objeto la regulación de la obligación de los operadores de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación, así como el deber de cesión de dichos datos a los agentes facultados, siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales.

Esta Ley se aplica a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o usuario registrado. Se excluye del ámbito de aplicación de la citada Ley el contenido de las comunicaciones electrónicas, incluida la información consultada utilizando una red de comunicaciones electrónicas.

La Ley 25/2007, de 18 de octubre, enumera en su artículo 3, de manera precisa y detallada, el listado de datos que quedan sujetos a la obligación de conservación en el marco de las comunicaciones por telefonía fija, móvil o Internet. Estos datos son los necesarios para identificar el origen y destino de la comunicación, su hora, fecha y duración, el tipo de servicio utilizado y el equipo de comunicación de los usuarios utilizado y, en el caso de utilización de un equipo móvil, los datos necesarios para su localización. En aplicación de las previsiones contenidas en la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, quedan incluidas también en el ámbito de aplicación de la Ley las denominadas llamadas telefónicas infructuosas. Igualmente se incluye la obligación de conservar los elementos que sean suficientes para identificar el momento de activación de los teléfonos que funcionen bajo la modalidad de prepago.

La disposición adicional única de la Ley 25/2007, de 18 de octubre, a los efectos de poder establecer instrumentos para controlar el empleo para fines delictivos de los equipos de telefonía móvil adquiridos mediante la modalidad de prepago, establece, como obligación

de los operadores que comercialicen dicho servicio, la llevanza de un registro con la identidad de los compradores.

Asimismo, la citada Ley 25/2007, de 18 de octubre, establece en su disposición final cuarta, relativa al formato de entrega de los datos, que la cesión a los agentes facultados de los datos cuya conservación sea obligatoria, se efectuará en formato electrónico, en la forma que se determine por Orden conjunta de los Ministros de Interior, de Defensa y de Economía y Hacienda. La citada habilitación normativa a favor del Ministerio de Defensa debe entenderse residenciada actualmente en el Ministerio de la Presidencia, puesto que el Centro Nacional de Inteligencia, del cual se deriva su afección, ha pasado a depender de este último Departamento, en virtud de lo establecido en la disposición adicional segunda del Real Decreto 1823/2011, de 21 de diciembre, por el que se reestructuran los Departamentos Ministeriales. Y por idénticos motivos de reestructuración orgánica, la referencia al Ministerio de Economía y Hacienda deba entenderse encuadrada en el ámbito competencial del Ministerio de Hacienda y Administraciones Públicas.

Esta Orden tiene por objeto el establecimiento de las especificaciones técnicas del formato de entrega a los agentes facultados de los datos conservados por los operadores que son generados y tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación.

Se adopta el modelo promovido por el ETSI (Instituto Europeo de Normalización de las Telecomunicaciones) para el establecimiento de dichas especificaciones. Este modelo consiste en un conjunto de normas elaboradas en el seno de este organismo de normalización en el que participan expertos de todos los sectores involucrados en la retención de datos, lo que garantiza un elevado nivel de consenso y de calidad de las normas desarrolladas, así como el mantenimiento y la adaptación a las diferentes tecnologías de telecomunicaciones que vayan surgiendo en el mercado.

La adopción del modelo ETSI implica la incorporación a la legislación española de una especificación técnica del ETSI que especifica el flujo de información así como los procedimientos, formatos y protocolos específicos de las interfaces de entrega (HI) entre los sujetos obligados y los agentes facultados: ETSI TS 102 657.

Finalmente, la presente Orden ha sido sometida al previo informe de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto en los artículos 37.h) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y 5.b) del Estatuto de la Agencia, aprobado por el Real Decreto 428/1993, de 26 de marzo.

En su virtud, a propuesta de este Ministerio y de los Ministros del Interior, de Hacienda y Administraciones Públicas, dispongo:

Artículo 1. *Objeto y ámbito de aplicación.*

Constituye el objeto de esta orden el establecimiento de las especificaciones técnicas del formato de entrega a los agentes facultados de los datos objeto de conservación a que hace referencia el artículo 3 y la disposición adicional única de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, de acuerdo con lo establecido en la disposición final cuarta de dicha Ley.

Lo dispuesto en esta orden se entiende sin perjuicio de los desarrollos reglamentarios previstos en la disposición final tercera de la mencionada Ley.

Estarán obligados a seguir los procedimientos y adoptar las medidas a las que se refiere la presente orden ministerial los operadores que presten o estén en condiciones de prestar servicios de comunicaciones electrónicas disponibles al público o de establecer o explotar redes públicas de comunicaciones en España, con independencia de la naturaleza, ámbito territorial y momento que tuvo efecto su habilitación, en los términos establecidos en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

Artículo 2. *Formato de entrega de los datos a los agentes facultados.*

1. Número de solicitudes individuales de cesión de datos entre todos los agentes facultados superior a 2.000.–En el marco de la Ley 25/2007, de 18 de octubre, la cesión a los agentes facultados de los datos cuya conservación sea obligatoria por parte de los operadores, se efectuará, cuando el número de solicitudes individuales de cesión de datos

entre todos los agentes facultados sea superior a 2.000 solicitudes durante el año natural anterior a la entrada en vigor de la presente orden ministerial, según el formato establecido en la especificación técnica del Instituto Europeo de Normalización de las Telecomunicaciones (ETSI) TS 102 657, Lawful Interception (LI); Retained data handling; Handover interface for the request and delivery of retained data, con las modificaciones y precisiones que se establecen en el anexo I de esta orden ministerial.

2. Número de solicitudes individuales de cesión de datos entre todos los agentes facultados igual o inferior a 2.000.–Cuando un sujeto obligado haya recibido un número de solicitudes individuales de cesión de datos entre todos los agentes facultados igual o inferior a 2.000 solicitudes durante el año natural anterior a la entrada en vigor de la presente orden ministerial, o en años naturales posteriores se viera disminuido el número de las mismas por debajo de las ya citadas 2.000 solicitudes, en lugar de utilizar el formato de entrega basado en la norma ETSI TS 102 657 podrá optar por utilizar otra solución tecnológica acordada previamente con los agentes facultados de entre los diferentes formatos especificados para este caso en el anexo III, en formato electrónico y cuyo nombre se adecuará a lo definido en el punto 7.1 del anexo I de esta Orden ministerial.

Para poder optar a esta solución, el sujeto obligado deberá comunicar a cada agente facultado que no se han superado en el año natural anterior las 2.000 solicitudes individuales y su petición de acogerse a la solución tecnológica alternativa previamente acordada. En todo caso la solución tecnológica acordada deberá garantizar el cumplimiento de las medidas de seguridad exigibles conforme a lo establecido en la normativa de protección de datos de carácter personal.

Si en el primer caso no se alcanzara el acuerdo preceptivo entre el sujeto obligado y los agentes facultados o si establecida la excepción contemplada en el segundo caso se superara posteriormente el número de 2.000 solicitudes, se aplicará lo establecido en el apartado 1 de este artículo.

3. Plazo de adopción del formato de entrega.–Cuando un sujeto obligado haya recibido un número superior a 2.000 solicitudes individuales de cesión de datos durante el año natural anterior a la entrada en vigor de la presente orden ministerial o acordada la excepción del apartado 2 de este artículo se superara posteriormente el número de 2.000 solicitudes dentro de un año natural, dispondrá del plazo fijado por la Ley 25/2007, de 18 de octubre, en su disposición final cuarta, para implantar el procedimiento de cesión basado en la norma ETSI TS 102 657 adoptado en esta orden. Dicho plazo se contabilizará desde la entrada en vigor de la presente orden ministerial en el primer caso y desde el momento en el que se supere el número de 2.000 solicitudes dentro de un año natural en el segundo.

Artículo 3. *Información de localización.*

Los sujetos obligados que presten servicios móviles deberán proveer la información de localización del terminal móvil solicitada, de acuerdo con lo establecido en el anexo I de esta orden.

Artículo 4. *Canales de comunicaciones entre sujetos obligados y agentes facultados.*

Existirán dos tipos de canales de comunicaciones entre cada sujeto obligado y cada agente facultado para la entrega de los datos solicitados: un canal para intercambio de información administrativa sobre peticiones/respuestas (Interfaz HI-A), y otro canal para transmitir los datos retenidos por el sujeto obligado (Interfaz HI-B). Estos dos canales «lógicos» podrán ser realizados sobre el mismo canal «físico» de enlace, y en cualquier caso se encontrarán, obligatoriamente, dentro del territorio nacional.

El anexo II de esta orden recoge las características y requisitos que deben cumplir ambos canales de comunicaciones así como los pormenores del abono del coste de las comunicaciones por parte de los agentes facultados.

Artículo 5. *Comunicación de información relacionada con la de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones entre sujetos obligados.*

1. La información relacionada con el mandamiento de la conservación de datos, relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, que se intercambie entre sujetos obligados, se limitará a la estrictamente necesaria para satisfacer las necesidades derivadas de la obligación de colaborar entre operadores para la realización de la misma. Los sujetos obligados garantizarán en todo momento la confidencialidad de la información transmitida o almacenada, no pudiendo ser utilizada para ningún otro fin. En todo caso conforme a las exigencias de la Ley 25/2007, de 18 de octubre, este intercambio de información en modo alguno podrá referirse a los datos de carácter personal respecto de los que existe la obligación de conservación y, en su caso, comunicación a los agentes facultados.

2. Las órdenes de cesión de los datos conservados y cualquier otra información importante para la seguridad del sistema de conservación, debe transmitirse mediante un canal seguro, según se define en el anexo II de esta orden.

Disposición transitoria única. *Plazo para el cumplimiento.*

Los sujetos obligados que estén prestando servicio a la entrada en vigor de la presente orden ministerial deberán cumplir las obligaciones establecidas en la misma en el plazo fijado por la Ley 25/2007, de 18 de octubre, en su disposición final cuarta, conforme a lo dispuesto en el artículo 2 de esta orden ministerial.

Aquellos sujetos obligados que inicien su actividad con posterioridad a la entrada en vigor de esta orden ministerial, deberán cumplir las obligaciones establecidas en esta orden ministerial desde el inicio de su actividad, pudiéndose acoger a lo dispuesto en el párrafo segundo del artículo 2 cuando se verifiquen dichas condiciones a la finalización del primer año natural completo desde el inicio de su actividad.

Disposición final primera. *Habilitación normativa.*

Se faculta a los titulares de la Secretaría de Estado de Seguridad, de la Secretaría de Estado Director del Centro Nacional de Inteligencia (CNI) y de la Secretaría de Estado de Hacienda para actualizar conjuntamente el contenido de los anexos de la presente Orden.

Disposición final segunda. *Impacto presupuestario en la Administración Pública.*

Las previsiones contenidas en esta orden no supondrán incremento de gastos de personal por ningún concepto y se llevarán a cabo con los medios personales disponibles en los departamentos ministeriales y organismos interesados.

Disposición final tercera. *Entrada en vigor.*

La presente orden ministerial entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

ANEXOS

[Anexos I, II y III omitidos. Consúltese el PDF oficial.]

§ 45

Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación

Jefatura del Estado
«BOE» núm. 76, de 30 de marzo de 2022
Última modificación: 20 de diciembre de 2023
Referencia: BOE-A-2022-4973

Desde su introducción generalizada a finales de los años 90 del siglo XX, las redes móviles han sido un pilar del progreso de las telecomunicaciones y base para la introducción de las tecnologías de la información en todos los ámbitos de la sociedad, gracias tanto a la gradual extensión de su cobertura como, muy fundamentalmente, al desarrollo de nuevas capacidades que han incorporado las sucesivas generaciones de servicios móviles.

La más reciente de ellas, conocida como quinta generación o 5G, puede dar a las comunicaciones móviles e inalámbricas una nueva dimensión al integrar computación en la red, permitir crear redes virtuales, ofrecer baja latencia y prestar servicios de enorme valor añadido para la sociedad en ámbitos como el de la medicina, el transporte y la energía. Por eso, la Unión Europea y España impulsan el rápido despliegue de redes y la realización de proyectos demostrativos de su utilidad para distintos sectores.

La prestación de servicios avanzados para la población y la industria con apoyo en la tecnología se irá conformando como una realidad a lo largo de los próximos cinco o diez años. Pero, para que las redes 5G desarrollen el potencial que encierran es preciso generar la confianza necesaria en su funcionamiento continuado y en su protección frente a fugas o manipulaciones de datos o comunicaciones. Sin esa confianza, las personas y entidades que pueden aprovechar las oportunidades que ofrecen las redes 5G no harán uso de ellas, y la tecnología 5G no producirá los beneficios que se esperan de ella.

Las redes y servicios 5G poseen ventajas comparativas en seguridad respecto a las de generaciones precedentes. Pero presentan también riesgos específicos derivados por ejemplo de su arquitectura de red más compleja, abierta y desagregada, y de su capacidad para transportar ingentes volúmenes de información y permitir la interacción simultánea de múltiples personas y cosas. Su interconexión con otras redes y el carácter transnacional de muchas de las amenazas inciden en su seguridad, y el previsible empleo generalizado de estas redes para funciones esenciales para la economía y la sociedad, incrementará el impacto potencial de los incidentes de seguridad que sufran.

Los equipos y programas informáticos cobran una importancia singular en las redes 5G pues sus prestaciones características, como la computación en el borde (*edge computing*) o la virtualización múltiple de redes (*network slicing*), se orientan hacia paradigmas propios de la informática y los servicios de computación en nube, apartándose del enfoque tradicional de las arquitecturas de las redes de comunicaciones electrónicas. El funcionamiento de estas redes dependerá en gran medida de sistemas informáticos y de servicios

proporcionados por proveedores externos a los operadores (designados colectivamente en este real decreto-ley como «suministradores»), creándose una dependencia de éstos que podría aumentar el nivel de riesgo al que se está expuesto.

La arquitectura de las redes 5G anteriormente descrita y los nuevos requisitos de seguridad, conllevan la necesaria evolución de las estrategias tradicionales, que se basaban en garantizar su disponibilidad, confidencialidad e integridad frente a ataques provenientes del exterior.

La complejidad técnica y el nuevo paradigma tecnológico que implica la inclusión y generalización en el mercado de las telecomunicaciones y en otros muchos sectores económicos de la tecnología 5G, hace que los retos de seguridad que se plantean alrededor de las redes 5G no puedan abordarse en su totalidad con las normas sobre seguridad e integridad de las redes de comunicaciones electrónicas contenidas en la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, ni con el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, ni con la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

La materia regulada requiere una norma con rango de ley, ya que establece algunas obligaciones a empresas y potestades administrativas que deben establecerse por ley. Justifican esas limitaciones y potestades la importancia para la sociedad de la garantía del funcionamiento ordinario de servicios esenciales que podrían depender en un futuro de las redes y servicios 5G. La apertura de la red a multitud de usos y aplicaciones aumenta los puntos de ataque a la red, y la importancia del papel de los suministradores en su arquitectura y gestión aconseja tomar precauciones para evitar posibles incidentes atribuibles a su actuación.

A este respecto, se somete a los suministradores a estrictos controles de seguridad para garantizar su fiabilidad técnica y su independencia de injerencias externas, lo que da lugar a análisis de riesgos y medidas que realizarán los operadores y el Gobierno.

En el aspecto técnico, se da preeminencia a la aplicación de estándares internacionales y europeos y a los esquemas de certificación europeos que resulten de la ejecución del Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre Ciberseguridad. Además, los operadores deberán poner en marcha una estrategia de diversificación de suministradores para minimizar los riesgos e impacto de contingencias que les afecten.

En el ámbito estratégico, se examinará el perfil de riesgo de los suministradores más importantes de los operadores de redes y servicios 5G en España, en particular, desde el punto de vista de su protección frente a ataques y de su exposición a injerencias externas; pudiendo llegar a identificarse usuarios específicos o funciones restringidas de las redes donde no puedan actuar suministradores calificados como de alto riesgo o de riesgo medio.

Para crear y reforzar la industria de 5G en España, se impulsará la investigación, desarrollo e innovación en torno a la tecnología 5G, también en lo que a la ciberseguridad 5G se refiere.

El presente real decreto-ley establece normas especiales o adicionales a las existentes en otras leyes aplicables en materia de seguridad, incluidas la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, la Ley 36/2015, de 28 de septiembre, de seguridad nacional, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos (Reglamento general de protección de datos personales), la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales, o el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

En la elaboración de este real decreto-ley se ha tenido en cuenta la Recomendación (UE) 2019/534, de 26 de marzo de 2019, de la Comisión Europea, sobre la ciberseguridad de las redes 5G, el análisis de riesgos coordinado de los Estados miembros y la «caja de herramientas» acordada por éstos como base común para un desarrollo seguro de la tecnología 5G en Europa. Se incluyen en este real decreto-ley las recomendaciones fundamentales que la Comunicación de 29 de enero de 2020 de la Comisión Europea «Despliegue seguro de la 5G en la UE - Aplicación de la caja de herramientas de la UE»

(COM/2020/50 final) realizaba a los Estados miembros sobre la utilización de la «caja de herramientas».

El artículo 86 de la Constitución permite al Gobierno dictar decretos-leyes «en caso de extraordinaria y urgente necesidad», siempre que no afecten al ordenamiento de las instituciones básicas del Estado, a los derechos, deberes y libertades de los ciudadanos regulados en el título I de la Constitución, al régimen de las Comunidades Autónomas ni al Derecho electoral general.

El Tribunal Constitucional ha declarado que la situación de extraordinaria y urgente necesidad que exige, como presupuesto habilitante, el artículo 86.1 de la Constitución Española, puede deducirse «de una pluralidad de elementos», entre ellos, «los que quedan reflejados en la exposición de motivos de la norma» (STC 6/1983, de 4 de febrero),

En este sentido, la STC 61/2018, de 7 de junio (FJ 4), exige, por un lado, «la presentación explícita y razonada de los motivos que han sido tenidos en cuenta por el Gobierno para su aprobación», y por otro, «la existencia de una necesaria conexión entre la situación de urgencia definida y la medida concreta adoptada para subvenir a ella».

En todo caso, el Tribunal Constitucional exige para la utilización de este tipo de norma que la situación que se pretenda regular se ajuste al «juicio político o de oportunidad que corresponde al Gobierno» (STC 182/1997, de 30 de octubre).

Por todo ello, de acuerdo con la jurisprudencia del Tribunal Constitucional, a continuación, se concretan las razones que justifican la extraordinaria y urgente necesidad de incorporar al ordenamiento jurídico español, mediante real decreto-ley, las recomendaciones contenidas en la «caja de herramientas» de la Unión Europea en materia de Ciberseguridad 5G, a través de la aprobación del presente real decreto-ley sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación.

El 24 de febrero de 2022, las fuerzas armadas rusas iniciaron una agresión a gran escala de Ucrania desde Rusia, desde Bielorrusia y desde zonas no controladas por el Gobierno de Ucrania. Como consecuencia de ello, importantes zonas del territorio ucraniano se han convertido en zonas de conflicto armado.

El Consejo Europeo condenó con la máxima firmeza en sus Conclusiones de 24 de febrero de 2022 la agresión militar de Rusia contra Ucrania e hizo hincapié en que supone una grave violación del Derecho internacional y de los principios de la Carta de las Naciones Unidas. El Consejo Europeo exigió a Rusia que respetase plenamente la integridad territorial, la soberanía y la independencia de Ucrania dentro de sus fronteras reconocidas internacionalmente, lo que incluye el derecho de Ucrania a elegir su propio destino. En solidaridad con Ucrania, el Consejo Europeo acordó sanciones adicionales, pidió que prosiguiera la labor relativa a la preparación en todos los niveles e invitó a la Comisión Europea a que presentara medidas de emergencia.

Como consecuencia, el conflicto está provocando importantes implicaciones para la Unión Europea, entre las que se encuentra el incremento considerable del riesgo de ciberataques por motivos geoestratégicos, al que ya se refería el informe «Panorama de amenazas 2021», publicado por la Agencia de la Unión Europea para la Ciberseguridad (ENISA) en octubre de 2021.

Los días 14 de enero, 15 de febrero y 23 de febrero de 2022, se han constatado ciberataques que han afectado gravemente a servicios gubernamentales y bancarios de Ucrania. Asimismo, en las últimas semanas, se han recibido diversas alertas de la Agencia de Ciberseguridad e Infraestructuras (CISA) de Estados Unidos, que destacan la necesidad de reforzar la protección de los países europeos frente a posibles ciberamenazas.

En consecuencia, teniendo en cuenta la situación de conflicto internacional derivada de la agresión contra Ucrania y el elevado riesgo de ciberataques contra redes y servicios 5G ya desplegadas en nuestro país o con despliegue previsto para los próximos meses, dentro de ese «juicio político o de oportunidad» que, de acuerdo con la citada STC 182/1997, de 30 de octubre, corresponde al Gobierno, se considera que concurren las razones de extraordinaria y urgente necesidad a las que se refiere el artículo 86 de la Constitución Española para la tramitación del presente proyecto como real decreto-ley.

Ello permitirá garantizar la entrada en vigor con celeridad de aquellas medidas que permiten prohibir o limitar la actividad en el mercado de suministradores que hayan sido

considerados de alto riesgo o riesgo medio por el Gobierno, en base a criterios técnicos y aspectos estratégicos que pueden tener impacto en la seguridad, como el nivel de exposición a injerencias de terceros países, pudiendo llegar a identificarse usuarios específicos o funciones restringidas de las redes donde no puedan actuar estos suministradores calificados como de alto riesgo o riesgo medio.

En conclusión, se considera que el importante incremento del riesgo de ciberataques contra redes 5G desplegadas o a punto de ser desplegadas en nuestro país justifica la extraordinaria y urgente necesidad de adoptar cuanto antes medidas que, de acuerdo con lo establecido en la citada caja de herramientas, garanticen la ciberseguridad de la tecnología 5G y el refuerzo de la autonomía y soberanía tecnológica de la Unión Europea.

La aprobación de la llamada «Ley de Ciberseguridad 5G» (con la que identifica este real decreto-ley) está incluida como una de las reformas (Reforma C15R2) de la Componente 15 del Plan de Recuperación, Transformación y Resiliencia dedicado a «Conectividad digital, impulso de la ciberseguridad y despliegue del 5G», estando, en concreto, prevista como Hito CID 235 «la entrada en vigor de la Ley de Ciberseguridad 5G».

Se cumple el principio de necesidad, pues este real decreto-ley se dicta para garantizar un bien de interés general, como es la seguridad y confianza en las comunicaciones electrónicas; es conforme con el principio de proporcionalidad ya que las medidas son adecuadas a los riesgos identificados en cada caso; se ajusta al principio de seguridad jurídica porque se reconoce el marco normativo vigente en materia de seguridad y solo se añaden requisitos y controles adecuados a la singularidad de las redes y servicios 5G y sus riesgos. Se respeta el principio de transparencia ya que los interesados han podido participar en el procedimiento de elaboración de un borrador de anteproyecto de ley previo. Por último, cumple el principio de eficiencia pues se han limitado las cargas administrativas al mínimo imprescindible para conseguir el fin perseguido de la seguridad.

En su virtud, haciendo uso de la autorización contenida en el artículo 86 de la Constitución Española, a propuesta de la Ministra de Asuntos Económicos y Transformación Digital, y previa deliberación del Consejo de Ministros en su reunión del día 29 de marzo de 2022,

DISPONGO:

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

Este real decreto-ley establece requisitos de seguridad para la instalación, el despliegue y la explotación de redes de comunicaciones electrónicas y la prestación de servicios de comunicaciones electrónicas e inalámbricas basados en la tecnología de quinta generación (5G).

Artículo 2. *Objetivos.*

Este real decreto-ley persigue los siguientes objetivos:

a) Impulsar una seguridad integral del ecosistema generado por la tecnología 5G.

b) Reforzar la seguridad en la instalación y operación de las redes de comunicaciones electrónicas 5G y en la prestación de los servicios de comunicaciones móviles e inalámbricas que se apoyen en las redes 5G.

c) Promover un mercado de suministradores en las redes y servicios de comunicaciones electrónicas 5G suficientemente diversificado en aras de garantizar la seguridad basada en razones técnicas, estratégicas y operativas y evitar, por dichas razones, la presencia de suministradores con una calificación de alto riesgo o de riesgo medio en determinados elementos de red o ámbitos.

d) Reforzar la protección de la seguridad nacional.

e) Fortalecer la industria y fomentar las actividades de I+D+i nacionales en ciberseguridad relacionadas con la tecnología 5G.

Artículo 3. *Definiciones.*

1. A los efectos de este real decreto-ley, se entenderá por:

a) «Operador 5G»: la persona física o jurídica que instala, despliega o explota redes públicas 5G o presta servicios 5G disponibles al público a través, total o parcialmente, de las redes 5G, disponga de red 5G propia o no, y ha notificado al Registro de operadores el inicio de su actividad o está inscrita en el Registro de operadores.

b) «Redes 5G» o «redes basadas en la tecnología 5G»: el conjunto integrado de elementos o infraestructuras de red, ya sean *hardware* o *software*, sistemas de transmisión, equipos de conmutación o encaminamiento y demás recursos, incluidos los recursos asociados e infraestructuras digitales, que permitan el transporte de señales con los que proporcionar conectividad móvil e inalámbrica y, a través de ella, prestar servicios de comunicaciones electrónicas e inalámbricas a usuarios y empresas con características avanzadas, que incorporen las funciones y capacidades y respondan a los casos de utilización recogidos en la Recomendación UIT-R M.2083, de la Unión Internacional de Telecomunicaciones, o en el estándar técnico de la organización 3GPP (*3rd Generation Partnership Project*: Proyecto de Colaboración para la Tercera Generación).

Estas características avanzadas son, entre otras, la computación integrada en la red, transmisión de grandes volúmenes de datos a alta velocidad, mínima latencia en las comunicaciones, alta fiabilidad y capacidad para conectar un número masivo de dispositivos a la red o la provisión de servicios específicos para determinados usos o aplicaciones.

Se considera que forman parte de las redes 5G la totalidad de los elementos de red, infraestructuras, recursos y funciones de las redes empleadas para ofrecer servicios con las capacidades señaladas, aun cuando también sean usados en las redes y servicios de comunicaciones electrónicas de generaciones móviles precedentes.

c) «Riesgo»: toda circunstancia o hecho razonablemente identificable que tenga un posible efecto adverso en la seguridad de las redes y servicios 5G.

d) «Seguridad»: la capacidad de las redes y servicios 5G de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de dichas redes y servicios, de los datos almacenados, procesados o transmitidos, o de los servicios accesibles a través de ellos.

e) «Servicios 5G»: los servicios de comunicaciones electrónicas e inalámbricas, en los términos definidos en la Directiva 2018/1972, de 11 de diciembre de 2018, del Parlamento Europeo y del Consejo, por la que se establece el Código Europeo de las Comunicaciones Electrónicas, sus servicios asociados y otros servicios conexos dirigidos a proporcionar funcionalidades y operatividad a los anteriores, como el almacenamiento en la nube (*cloud computing*) o la computación en el borde (*edge computing*), en cuya prestación se emplean redes 5G.

f) «Suministrador 5G»: el fabricante, el representante autorizado, el importador, el distribuidor, el prestador de servicios logísticos o cualquier otra persona física o jurídica sujeta a obligaciones en relación con la fabricación de productos, su comercialización o su puesta en servicio en materia de equipos de telecomunicación, los suministradores de *hardware* y *software* y los proveedores de servicios auxiliares que intervengan en el funcionamiento u operación de redes 5G o en la prestación de servicios 5G.

g) «Usuario corporativo 5G»: la persona física o jurídica que instala, despliega o explota redes privadas 5G o presta servicios 5G a través, total o parcialmente, de las redes 5G, para fines profesionales o en autoprestación.

2. Serán de aplicación, asimismo, las definiciones establecidas en la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, y en el Código Europeo de las Comunicaciones.

Artículo 4. *Ámbito de aplicación.*

Este real decreto-ley se aplica a:

a) Los operadores 5G.
b) Los suministradores 5G.

c) Los usuarios corporativos 5G que tengan otorgados derechos de uso del dominio público radioeléctrico para instalar, desplegar o explotar una red privada 5G o prestar servicios 5G para fines profesionales o en autoprestación.

Artículo 5. *Tratamiento integral de la seguridad.*

1. Los sujetos previstos en el artículo 4 deberán llevar a cabo un tratamiento integral de la seguridad de las redes, elementos, infraestructuras, recursos, facilidades y servicios de los que sean responsables, para lo cual deberán llevar a cabo, mediante un método holístico, un análisis de las vulnerabilidades, amenazas y riesgos que les afecten como agentes económicos y de los componentes anteriormente relacionados, así como una gestión adecuada e integral de dichos riesgos mediante la utilización de las técnicas y medidas que sean adecuadas para lograr su mitigación o eliminación y alcanzar el objetivo final de una explotación y operación seguras de las redes y servicios 5G.

A tal efecto, los sujetos previstos en el artículo 4 deberán dar debido cumplimiento a lo dispuesto en este real decreto-ley, a lo que se establezca en el Esquema Nacional de Seguridad de redes y servicios 5G y a los actos que se dicten en ejecución de ambas disposiciones.

2. Para alcanzar este tratamiento integral de la seguridad, los sujetos previstos en el artículo 4 deberán proporcionar la información que sea necesaria en virtud de lo dispuesto en este real decreto-ley o en el Esquema Nacional de Seguridad de redes y servicios 5G o la que le sea requerida por el Ministerio de Asuntos Económicos y Transformación Digital en ejercicio de las funciones que se les asignan en este ámbito.

Dicha información tiene la consideración de confidencial, de forma que la misma no podrá ser utilizada para una finalidad distinta del cumplimiento de los objetivos y obligaciones establecidas en este real decreto-ley, en el Esquema Nacional de Seguridad de redes y servicios 5G y en los actos que se dicten en ejecución de ambas disposiciones.

3. El Esquema Nacional de Seguridad de redes y servicios 5G llevará a cabo igualmente un tratamiento integral de la seguridad de las redes y servicios 5G, considerando al efecto las aportaciones al alcance de cada agente de la cadena de valor de 5G, así como la normativa, las recomendaciones y los estándares técnicos de la Unión Europea, de la Unión Internacional de Telecomunicaciones (UIT) y de otras organizaciones internacionales, con el fin de garantizar el objetivo último de una explotación y operación seguras de las redes y servicios 5G en nuestro país.

CAPÍTULO II

Análisis de riesgos

Artículo 6. *Análisis de riesgos por los operadores 5G.*

1. Los operadores 5G deberán analizar los riesgos de las redes y servicios 5G, detectando vulnerabilidades y amenazas que les afecten tanto como agente económico como por los elementos de red, infraestructuras, recursos, facilidades y servicios que empleen o provean en la instalación, despliegue y explotación de redes 5G o en la prestación de servicios 5G.

2. Los operadores 5G que sean titulares o gestionen elementos de red de una red pública 5G, en su análisis de riesgos, deberán llevar a cabo un estudio pormenorizado e individualizado de las amenazas y vulnerabilidades que afecten, al menos, a los siguientes elementos, infraestructuras y recursos de una red pública 5G:

a) Los relativos a las funciones del núcleo de la red.
b) Las funciones de transporte y transmisión.
c) La red de acceso.
d) Los sistemas de control y gestión y los servicios de apoyo.
e) Las funciones de computación en el borde, virtualización de red y gestión de sus componentes.
f) Los relativos a intercambios de tráfico con redes externas e Internet.

g) Otros componentes y funciones que, a tal efecto, se determinen en el Esquema Nacional de Seguridad de redes y servicios 5G.

3. Son elementos críticos de una red pública 5G:

a) Los relativos a las funciones del núcleo de la red.
b) Los sistemas de control y gestión y los servicios de apoyo.
c) La red de acceso en aquellas zonas geográficas y ubicaciones que se determine.

4. El análisis de riesgos que lleve a cabo un operador 5G deberá tener en cuenta, al menos, los siguientes factores:

a) Parametrización y configuración de elementos y funciones de red.
b) Políticas de integridad y actualización de los programas informáticos.
c) Estrategias de permisos de acceso a activos físicos y lógicos.
d) Dependencias de determinados suministradores en elementos críticos de la red 5G.
e) Agentes externos, incluyendo grupos organizados con capacidad para atacar la red.
f) Equipos terminales y dispositivos conectados a la red.
g) Elementos de usuarios corporativos y redes externas conectadas a la red 5G.
h) La interrelación con otros servicios esenciales para la sociedad.

5. A fin de llevar a cabo un tratamiento integral de la seguridad de las redes y servicios 5G, el operador 5G deberá recabar de sus suministradores las prácticas y medidas de seguridad que se han adoptado en los productos y servicios que les han suministrado, teniendo en cuenta los factores de riesgo indicados en este capítulo y el perfil de riesgo del suministrador. Esta información deberá ser proporcionada por los suministradores y su tratamiento será confidencial, de manera que sólo podrá ser utilizada por los operadores 5G para efectuar un análisis y gestión de riesgos y por el Ministerio de Asuntos Económicos y Transformación Digital y los demás organismos públicos competentes para la aplicación de lo dispuesto en este real decreto-ley a los exclusivos fines del mismo.

6. El análisis de riesgos del operador 5G deberá incluir una priorización y jerarquía de los riesgos en función de los siguientes parámetros:

a) Afectación a un elemento crítico de la red pública 5G.
b) Tipo de recurso, infraestructura y servicio que pueda verse afectado.
c) Afectación a la integridad y mantenimiento técnico de la red o a la continuidad del servicio.
d) Capacidad de detección y recuperación.
e) Número y tipo de usuarios afectados.
f) Tipo de información cuya integridad haya podido verse comprometida.

7. El análisis de riesgos por el operador 5G debe ser llevado a cabo cada dos años y ser remitido al Ministerio de Asuntos Económicos y Transformación Digital.

Artículo 7. *Análisis de riesgos por los suministradores 5G.*

1. Los suministradores 5G deben analizar los riesgos de los equipos de telecomunicación, *hardware* y *software* y servicios auxiliares que intervengan en el funcionamiento u operación de redes 5G o en la prestación de servicios 5G, detectando vulnerabilidades y amenazas que le afecten tanto a la gestión de la empresa como a dichos equipos, *hardware*, *software* y servicios.

2. Los suministradores 5G deberán aportar este análisis de riesgos al Ministerio de Asuntos Económicos y Transformación Digital, cuando sea requerido para ello.

3. No obstante lo dispuesto en el apartado anterior, los suministradores 5G que hayan sido calificados de alto riesgo o de riesgo medio deberán remitir al Ministerio de Asuntos Económicos y Transformación Digital un análisis de riesgos de sus equipos, productos o servicios involucrados en las redes y servicios 5G en el plazo de seis meses a contar desde que hayan sido calificados de alto riesgo o de riesgo medio.

4. Los suministradores 5G que sean calificados de alto riesgo o de riesgo medio deberán llevar a cabo el análisis de riesgos cada dos años y remitirlo al Ministerio de Asuntos Económicos y Transformación Digital.

Artículo 8. *Análisis de riesgos por los usuarios corporativos 5G.*

1. Los usuarios corporativos 5G que tengan otorgados derechos de uso del dominio público radioeléctrico para instalar, desplegar o explotar una red privada 5G o prestar servicios 5G para fines profesionales o en autoprestación deberán analizar los riesgos de las redes y servicios 5G, detectando vulnerabilidades y amenazas que afecten a los elementos de red, infraestructuras, recursos, facilidades y servicios que empleen o provean en la instalación, despliegue y explotación de redes privadas 5G o en la prestación de servicios 5G en autoprestación.

2. Los usuarios corporativos 5G mencionados en el apartado 1 deberán aportar este análisis de riesgos al Ministerio de Asuntos Económicos y Transformación Digital, cuando sea requerido para ello.

Artículo 9. *Factores de riesgo a analizar por los sujetos previstos en el artículo 4.*

El Esquema Nacional de Seguridad de redes y servicios 5G deberá identificar los factores de riesgo a analizar por los sujetos previstos en el artículo 4 en función de la evolución tecnológica, la incorporación de nuevos avances, funcionalidades y estándares tecnológicos, la situación del mercado de comunicaciones electrónicas y del de suministros y de la aparición de nuevas amenazas y vulnerabilidades.

Artículo 10. *Confidencialidad de la información sobre análisis de riesgos.*

El Ministerio de Asuntos Económicos y Transformación Digital podrá recabar de los sujetos previstos en el artículo 4 la información necesaria para el análisis de riesgos.

La información que los referidos sujetos proporcionen sobre el análisis de riesgos tiene la consideración de confidencial, de forma que la misma no podrá ser utilizada para una finalidad distinta del cumplimiento de los objetivos y obligaciones establecidas en este real decreto-ley, en el Esquema Nacional de Seguridad de redes y servicios 5G y en los actos que se dicten en ejecución de ambas disposiciones.

CAPÍTULO III

Gestión de los riesgos

Artículo 11. *Deber de gestionar los riesgos de seguridad.*

Los sujetos previstos en el artículo 4 deberán adoptar medidas técnicas y de organización adecuadas para gestionar los riesgos existentes en la instalación, despliegue y explotación de redes 5G y en la prestación de servicios 5G, con base en lo establecido en este real decreto-ley, en el Esquema Nacional de Seguridad de redes y servicios 5G y en los actos que se dicten en ejecución de ambas disposiciones.

Artículo 12. *Gestión de seguridad por los operadores 5G.*

1. Los operadores 5G deberán garantizar la instalación, despliegue y explotación seguros de redes públicas 5G y la prestación segura de servicios 5G disponibles al público mediante la aplicación de técnicas y procedimientos de operación y supervisión que garanticen la seguridad de redes y servicios 5G, así como el cumplimiento de lo establecido en este real decreto-ley.

2. Los operadores 5G tienen las siguientes obligaciones de seguridad dirigidas a mitigar riesgos:

a) Adoptar medidas técnicas y operativas para garantizar la integridad física y lógica de las redes 5G o cualesquiera de sus elementos, infraestructuras y recursos, así como la continuidad en la prestación de servicios 5G.

b) Adoptar planes y medidas de contingencia específicas para asegurar la continuidad de otros servicios esenciales para la sociedad que dependan de las redes y servicios 5G.

c) Seleccionar e identificar a las personas que puedan acceder a los activos físicos y lógicos de la red, y realizar el mantenimiento de registros de acceso.

d) Mantener las credenciales de usuario para el acceso a la red en posesión del operador.

e) Utilizar únicamente productos, recursos, servicios o sistemas certificados para la operación de las redes 5G, o en alguna de sus partes o elementos.

f) Cumplir las normas o especificaciones técnicas aplicables a redes y sistemas de información.

g) Cumplir con los esquemas europeos de certificación de productos, servicios o sistemas, sean o no específicos de la tecnología 5G, que se empleen en la operación o explotación de redes y servicios 5G.

h) Someterse, a su costa, a una auditoría de seguridad realizada por una entidad pública o una entidad privada acreditada a estos efectos.

i) Exigir a sus suministradores el cumplimiento de estándares de seguridad, desde el diseño de los productos y servicios hasta su puesta en funcionamiento.

j) Controlar su propia cadena de suministro y la estrategia de diversificación que haya diseñado.

3. En particular, los operadores 5G que sean titulares o exploten elementos críticos de una red pública 5G tienen adicionalmente las siguientes obligaciones:

a) Deberán diseñar una estrategia de diversificación en la cadena de suministro de los equipos de telecomunicación, sistemas de transmisión, equipos de conmutación o encaminamiento y demás recursos que permitan el transporte de señales en una red pública 5G, de forma que dichos equipos, sistemas o recursos sean proporcionados, como mínimo, por dos suministradores diferentes en la red de acceso. En el núcleo de la red y en los sistemas de control y gestión y los servicios de apoyo, el suministrador podrá ser único.

A estos efectos, se considera que los suministradores no son diferentes si todos ellos pertenecen al mismo grupo de empresas, conforme a los criterios establecidos en el artículo 42 del Código de Comercio.

b) No podrán utilizar en los elementos críticos de red equipos de telecomunicación, sistemas de transmisión, equipos de conmutación o encaminamiento y demás recursos, que permitan el transporte de señales, hardware, software o servicios auxiliares de suministradores que hayan sido calificados de alto riesgo.

c) No podrán utilizar en la red de acceso de una red pública 5G equipos de telecomunicación, sistemas de transmisión, equipos de conmutación o encaminamiento y demás recursos, que permitan el transporte de señales, hardware, software o servicios auxiliares de suministradores que hayan sido calificados de alto riesgo, en aquellas estaciones radioeléctricas con las que se proporcione cobertura a centrales nucleares, centros vinculados a la Defensa Nacional y las ubicaciones, áreas y centros que, por su vinculación a la seguridad nacional o al mantenimiento de determinados servicios esenciales para la comunidad o sectores estratégicos, sean determinados por el Consejo de Seguridad Nacional, previo informe del Ministerio de Transformación Digital. La determinación y difusión de estas ubicaciones serán tratadas como materias clasificadas conforme a la regulación establecida en la Ley 9/1968, de 5 de abril, sobre secretos oficiales.

d) Deberán solicitar y obtener del Ministerio de Transformación Digital autorización para la instalación, modificación o adaptación de estaciones radioeléctricas que proporcionen cobertura a estas ubicaciones, áreas y centros previamente determinados conforme a lo dispuesto en el párrafo anterior, habida cuenta de su vinculación con la seguridad nacional o el mantenimiento de determinados servicios esenciales para la comunidad o sectores estratégicos. En el otorgamiento de esta autorización, el Ministerio de Transformación Digital tendrá en cuenta los equipos de telecomunicación, sistemas de transmisión, equipos de conmutación o encaminamiento y demás recursos que permitan el transporte de señales, hardware, software o servicios auxiliares a instalar, las condiciones técnicas en el uso del dominio público radioeléctrico y las características intrínsecas y fines a proteger en esas ubicaciones, áreas y centros previamente determinados.

El plazo para el otorgamiento de estas autorizaciones es de tres meses, entendiéndose desestimada la solicitud en caso de ausencia de resolución expresa. La resolución, expresa o presunta, pone fin a la vía administrativa y es directamente recurrible ante la jurisdicción

contencioso-administrativa, sin perjuicio de que potestativamente se pueda interponer contra el mismo un recurso de reposición con carácter previo al recurso contencioso-administrativo.

e) Deberán ubicar los elementos críticos de una red pública 5G dentro del territorio nacional. No obstante, determinados elementos, funciones y sistemas tanto del núcleo de la red como de los sistemas de control y gestión y los servicios de apoyo podrán ubicarse fuera del territorio nacional, siempre y cuando el Ministerio de Transformación Digital pueda ejercer las facultades que le atribuye este real decreto-ley, en particular, las facultades de inspección y régimen sancionador previstas en el capítulo V, de manera que pueda efectuar una verificación integral sobre el funcionamiento, operatividad y condiciones de uso de dichos elementos críticos de una red 5G y, en su caso, poder adoptar medidas, cautelares o definitivas, sobre dichos elementos, funciones y sistemas o el equipamiento utilizado en el ejercicio de estas facultades.

4. En el caso de que como consecuencia de operaciones de concentración empresarial, se redujera el número de suministradores incluidos en la estrategia de diversificación en la cadena de suministro que implicara que no se cumpliera el límite mínimo de dos suministradores diferentes establecido en el apartado 3.a) de este artículo, el operador 5G deberá comunicárselo al Ministerio de Asuntos Económicos y Transformación Digital, que impulsará que el Gobierno, mediante acuerdo adoptado en Consejo de Ministros, previa audiencia de los operadores 5G y suministradores 5G afectados, decida si resulta posible mantener un suministrador único, teniendo en cuenta las condiciones concretas de la operación de concentración empresarial, la situación del mercado de los suministradores, las alternativas de suministro de equipos y productos sustitutivos viables, la implantación de esos equipos y productos en la red 5G del operador, especialmente en los elementos críticos de la red 5G, la calificación del suministrador como de alto riesgo, la dificultad intrínseca para llevar a cabo la sustitución de equipos, los ciclos de actualización de equipos, la migración de las redes 5G no autónomas a autónomas, así como su impacto económico.

5. Los operadores 5G que sean titulares o exploten elementos críticos de una red pública 5G deberán remitir al Ministerio de Asuntos Económicos y Transformación Digital la estrategia de diversificación en la cadena de suministro en el plazo de seis meses a contar desde la entrada en vigor de este real decreto-ley.

Asimismo, la estrategia de diversificación en la cadena de suministro deberá ser remitida al Ministerio de Asuntos Económicos y Transformación Digital cada vez que sea objeto de modificación.

Igualmente, los operadores 5G que sean titulares o exploten elementos críticos de una red pública 5G deberán remitir al Ministerio de Asuntos Económicos y Transformación Digital información cada año sobre el estado de ejecución de la estrategia de diversificación en la cadena de suministro.

6. El Ministerio de Transformación Digital, si considera que no queda garantizada la continuidad en la prestación de los servicios 5G, la integridad física o lógica de la red 5G, que existe una amplia exposición al equipamiento instalado por un suministrador que en determinadas circunstancias puede poner en peligro la funcionalidad y operatividad de la red 5G o para garantizar la seguridad en la provisión de servicios utilizados por los servicios de Seguridad Nacional, Defensa Nacional o por distintas Administraciones Públicas, y teniendo en cuenta si existe calificación de suministradores de alto riesgo, las alternativas de suministro de equipos y productos sustitutivos viables, la implantación de esos equipos y productos en la red 5G del operador, especialmente en los elementos críticos de la red 5G, y los ciclos de actualización de equipos, podrá modificar la estrategia de diversificación en la cadena de suministro de un operador 5G.

Antes de aprobar la modificación, se deberá efectuar un trámite de audiencia con el operador 5G y suministrador o suministradores 5G afectados por un plazo de 15 días hábiles. La resolución pon fin a la vía administrativa y es directamente recurrible ante la jurisdicción contencioso-administrativa, sin perjuicio de que potestativamente se pueda interponer contra la misma un recurso de reposición con carácter previo al recurso contencioso-administrativo.

7. Los operadores 5G deberán remitir al Ministerio de Asuntos Económicos y Transformación Digital cada dos años una descripción de las medidas técnicas y organizativas diseñadas y aplicadas para gestionar y mitigar los riesgos.

Artículo 13. *Gestión de seguridad por los suministradores 5G.*

1. Los suministradores 5G deberán garantizar la seguridad de los equipos de telecomunicación, *hardware*, *software* o servicios auxiliares que proporcionen y que sean objeto de uso por las redes y servicios 5G.

2. Los suministradores 5G tienen las siguientes obligaciones de seguridad dirigidas a mitigar riesgos, las cuales serán objeto de concreción y desarrollo en el Esquema Nacional de Seguridad de redes y servicios 5G:

a) Cumplir estándares de seguridad desde el diseño de los equipos, productos y servicios hasta su puesta en funcionamiento.

b) Reforzar la integridad del *software*, actualización y gestión de parches.

c) Acreditar la certificación de productos y servicios de tecnologías de la información que se usen en las redes y servicios 5G.

d) Garantizar la aplicación de medidas de seguridad técnicas y organizativas estándar a través de un sistema de certificación.

e) Efectuar una auditoría de seguridad de sus equipos, productos y servicios.

f) Proporcionar información sobre posibles injerencias de terceros en el diseño, operación y funcionamiento de sus equipos, productos y servicios.

g) Colaborar con los operadores 5G y usuarios corporativos 5G proporcionando información y acreditando el cumplimiento de estándares de seguridad de equipos, productos y servicios que suministren.

3. Los suministradores 5G deberán aportar al Ministerio de Asuntos Económicos y Transformación Digital una descripción de las medidas técnicas y organizativas diseñadas y aplicadas para gestionar y mitigar los riesgos, cuando sean requeridos para ello.

4. No obstante lo dispuesto en el apartado anterior, los suministradores 5G que hayan sido calificados de alto riesgo o de riesgo medio deberán remitir al Ministerio de Asuntos Económicos y Transformación Digital un informe de las medidas técnicas y organizativas diseñadas y aplicadas para gestionar y mitigar los riesgos en el plazo de seis meses a contar desde que hayan sido calificados de alto riesgo o de riesgo medio.

5. Los suministradores 5G de alto riesgo y de riesgo medio deberán remitir al Ministerio de Asuntos Económicos y Transformación Digital cada dos años una descripción de las medidas técnicas y organizativas diseñadas y aplicadas para gestionar y mitigar los riesgos.

Artículo 14. *Suministradores 5G de alto riesgo y de riesgo medio.*

1. El Gobierno, mediante acuerdo adoptado en Consejo de Ministros, previo informe del Consejo de Seguridad Nacional y previa audiencia de los operadores 5G y suministradores 5G afectados por un plazo de 15 días hábiles, podrá calificar que determinados suministradores 5G son de alto riesgo.

A tal efecto, el Gobierno analizará tanto las garantías técnicas de funcionamiento y operatividad de sus equipos, productos y servicios como su exposición a injerencias externas.

2. En relación con el análisis de las medidas técnicas y las garantías técnicas de funcionamiento y operatividad de sus equipos, productos y servicios se valorará aspectos relativos al cumplimiento de normas o especificaciones técnicas, su verificación mediante esquemas de certificación, o la superación de pruebas o auditorías de seguridad realizadas por entidades independientes.

3. En relación con el análisis de las medidas estratégicas y exposición a injerencias externas, se valorarán los siguientes aspectos:

a) Los vínculos de los suministradores y de su cadena de suministro, con los gobiernos de terceros países.

b) La composición de su capital social y la estructura de sus órganos de gobierno.

c) El poder de un tercer Estado para ejercer presión sobre la actuación o ubicación de la empresa.

d) Las características de la legislación y la política de ciberdefensa y el respeto al derecho internacional y a las resoluciones y acuerdos de la Organización de las Naciones Unidas de ese tercer Estado.

e) Los acuerdos de cooperación en materia de seguridad, ciberseguridad, delitos cibernéticos o protección de datos firmados con el país tercero de que se trate, así como los tratados internacionales en esas materias de que sea parte dicho Estado.

f) El grado de adecuación de la normativa del tercer Estado sobre protección de datos personales a la de España, al Reglamento General de Protección de Datos aprobado por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, adoptada por la Unión Europea y a cualquier otra normativa aplicable en materia de seguridad de las redes y sistemas de información y de telecomunicaciones.

4. El acuerdo del Consejo de Ministros por el que se califique a determinados suministradores 5G como suministradores de alto riesgo determinará el plazo en que lo operadores 5G deberán llevar a cabo la sustitución de los equipos, productos y servicios proporcionados por dicho suministrador en la red y servicios del operador 5G, cuando ello fuera necesario, para lo cual deberá tener en cuenta la situación del mercado de los suministradores, las alternativas de suministro de equipos y productos sustitutivos viables, la implantación de esos equipos y productos en la red 5G del operador, especialmente en los elementos críticos de la red 5G y en función de cuáles son en concreto los elementos críticos afectados, la dificultad intrínseca para llevar a cabo la sustitución de equipos, los ciclos de actualización de equipos, la migración de las redes 5G no autónomas a autónomas, así como su impacto económico, si bien, en ningún caso, este plazo podrá ser inferior a un año.

5. El acuerdo del Consejo de Ministros por el que se califique que determinados suministradores 5G son de alto riesgo pone fin a la vía administrativa y es directamente recurrible ante la jurisdicción contencioso-administrativa, sin perjuicio de que potestativamente se pueda interponer contra el mismo un recurso de reposición con carácter previo al recurso contencioso-administrativo.

6. Los suministradores de alto riesgo cuyos equipos de telecomunicación, *hardware*, *software* o servicios auxiliares proporcionados sean utilizados única y exclusivamente en redes privadas 5G o para la prestación de servicios 5G en régimen de autoprestación son calificados como suministradores de riesgo medio.

Artículo 15. *Gestión de seguridad por los usuarios corporativos 5G.*

1. Los usuarios corporativos 5G que tengan otorgados derechos de uso del dominio público radioeléctrico para instalar, desplegar o explotar una red privada 5G o prestar servicios 5G para fines profesionales o en autoprestación deberán garantizar la instalación, despliegue y explotación seguros de redes privadas 5G y prestación segura de servicios 5G en autoprestación mediante la aplicación de técnicas y procedimientos de operación y supervisión que garanticen la seguridad de las redes y servicios 5G.

2. Los usuarios corporativos 5G mencionados deberán aportar al Ministerio de Asuntos Económicos y Transformación Digital una descripción de las medidas técnicas y organizativas diseñadas y aplicadas para gestionar y mitigar los riesgos, cuando sean requeridos para ello.

Artículo 16. *Condiciones de cumplimiento de las obligaciones.*

En el cumplimiento de las obligaciones establecidas en los artículos anteriores, los sujetos previstos en el artículo 4 tendrán en cuenta y aplicarán lo establecido en este real decreto-ley, en el Esquema Nacional de Seguridad de redes y servicios 5G y en los actos que se dicten en ejecución de ambas disposiciones.

Artículo 17. *Gestión de seguridad por las Administraciones públicas.*

1. Las administraciones públicas deberán adoptar medidas técnicas y de organización adecuadas para gestionar los riesgos existentes en la instalación, despliegue y explotación de redes 5G y en la prestación de servicios 5G.

2. En particular, las administraciones públicas que quieran llevar a cabo la instalación, despliegue y explotación de redes 5G, ya sean públicas o privadas, o la prestación de servicios 5G, disponibles al público o en autoprestación, no podrán, por razones de

seguridad nacional, utilizar equipos, productos y servicios proporcionados por suministradores de alto riesgo o riesgo medio.

Artículo 18. *Cumplimiento de la normativa sobre inversiones extranjeras y sobre competencia.*

Las obligaciones establecidas en los artículos anteriores se entienden sin perjuicio de la aplicación de los instrumentos de control sobre inversiones extranjeras directas en los sujetos previstos en el artículo 4 que sean de nacionalidad española, así como de la aplicación de la normativa en materia de defensa de la competencia.

Artículo 19. *Confidencialidad de la información sobre gestión de riesgos.*

El Ministerio de Asuntos Económicos y Transformación Digital podrá recabar de los sujetos previstos en el artículo 4 la información necesaria para la gestión de riesgos.

La información que los referidos sujetos proporcionen sobre sobre la gestión de riesgos tiene la consideración de confidencial, de forma que la misma no podrá ser utilizada para una finalidad distinta del cumplimiento de los objetivos y obligaciones establecidas en este real decreto-ley, en el Esquema Nacional de Seguridad de redes y servicios 5G y en los actos que se dicten en ejecución de ambas disposiciones.

CAPÍTULO IV

Esquema Nacional de Seguridad de redes y servicios 5G

Artículo 20. *Contenido del Esquema Nacional de Seguridad de redes y servicios 5G.*

1. El Esquema Nacional de Seguridad de redes y servicios 5G llevará a cabo un tratamiento integral y global de la seguridad de las redes y servicios 5G, considerando las aportaciones al alcance de cada agente de la cadena de valor de 5G para garantizar un funcionamiento continuado y seguro de la red y los servicios 5G.

2. En el Esquema Nacional de Seguridad de redes y servicios 5G se efectuará un análisis de riesgos a nivel nacional sobre la seguridad de las redes y servicios 5G así como identificará, concretará y desarrollará medidas a nivel nacional para mitigar y gestionar los riesgos analizados.

Artículo 21. *Aprobación y revisión del Esquema Nacional de Seguridad de redes y servicios 5G.*

1. El Gobierno aprobará, mediante real decreto, a propuesta del Ministerio de Asuntos Económicos y Transformación Digital, previo informe del Consejo de Seguridad Nacional, un Esquema Nacional de Seguridad de redes y servicios 5G.

2. El Esquema Nacional de Seguridad de redes y servicios 5G se revisará al menos cada cuatro años o cuando las circunstancias lo aconsejen.

Artículo 22. *Análisis de riesgos en el Esquema Nacional de Seguridad de redes y servicios 5G.*

1. El Esquema Nacional de Seguridad de redes y servicios 5G efectuará un análisis de riesgos a nivel nacional sobre la seguridad de las redes y servicios 5G.

2. En este análisis de riesgos nacional se identificarán, entre otros, los siguientes aspectos:

a) El análisis general de los riesgos de las redes y servicios 5G, tomando en consideración la información recabada de los sujetos previstos en el artículo 4.

b) El examen de las vulnerabilidades ligadas a la cadena de suministro de las redes y servicios 5G.

c) La evaluación del grado de dependencia de los suministradores del conjunto de las redes y servicios 5G en España teniendo en cuenta los análisis de riesgos y las estrategias de diversificación de suministradores remitidos por los operadores 5G, así como el riesgo de

interrupción del suministro por circunstancias económicas, societarias o comerciales que afecten a los suministradores.

d) La evaluación de la eficacia de las medidas de seguridad aplicadas hasta la aprobación de cada análisis de riesgos nacional para mitigar los riesgos puestos de manifiesto por tal análisis.

3. El Esquema Nacional de Seguridad de redes y servicios 5G establecerá una jerarquía de riesgos en función de los análisis de riesgos llevados a cabo por los sujetos previstos en el artículo 4 y en función de las deficiencias apreciadas en la evaluación de la eficacia de las medidas aplicadas.

Artículo 23. *Gestión de riesgos en el Esquema Nacional de Seguridad de redes y servicios 5G.*

1. En el Esquema Nacional de Seguridad de redes y servicios 5G se establecerán, concretarán y desarrollarán criterios, requisitos, condiciones y plazos para que los sujetos previstos en el artículo 4 puedan dar cumplimiento a las obligaciones que a cada una de estas categorías de agentes económicos les impone este real decreto-ley.

Para ello, se tendrá en cuenta el análisis de riesgos nacional que incorpora la propia Estrategia Nacional y la evaluación de la eficacia de las medidas aplicadas con anterioridad por los sujetos previstos en el artículo 4 para mitigar y gestionar los riesgos en las redes y servicios 5G.

2. En el Esquema Nacional de Seguridad de redes y servicios 5G se podrá supeditar la utilización de un equipo, programa o servicio en concreto por un operador 5G, suministrador 5G o usuario corporativo 5G previsto en el artículo 4 a la previa obtención de una certificación establecida en virtud del Reglamento (UE) 2019/881, del Parlamento europeo y del Consejo, de 17 de abril de 2019, sobre la ciberseguridad.

3. El Esquema Nacional de Seguridad de redes y servicios 5G, al margen de las estrategias de diversificación de la cadena de suministro que puedan tener los operadores 5G, podrá llevar a cabo un análisis específico y podrá proponer objetivos de diversificación de suministradores 5G en la cadena de suministro en las redes y servicios 5G para el conjunto del Estado, para lo cual podrá arbitrar medidas objetivas, proporcionadas y no discriminatorias dirigidas al cumplimiento de estos objetivos, siempre dentro del marco establecido en este real decreto-ley.

4. El Esquema Nacional de Seguridad de redes y servicios 5G también contendrá medidas para mitigar o gestionar los riesgos derivados del mercado de equipos terminales y dispositivos conectados.

La fabricación, importación, distribución, puesta en el mercado y comercialización de equipos terminales y dispositivos para conectarse a una red 5G y poder prestar servicios 5G, estará condicionado al cumplimiento de los requisitos esenciales aplicables relacionados con la ciberseguridad, adoptados conforme a la normativa europea, en particular, en relación con la protección de los datos personales, la privacidad, y la protección contra el fraude.

Artículo 24. *Deber de colaboración en la aprobación y ejecución del Esquema Nacional de Seguridad de redes y servicios 5G.*

Todos los sujetos previstos en el artículo 4, así como los fabricantes, importadores, distribuidores y quienes pongan en el mercado y comercialicen equipos terminales y dispositivos para conectarse a una red 5G y poder prestar servicios 5G deberán prestar la colaboración y remitir la información que le sea requerida para la elaboración, aprobación y ejecución del Esquema Nacional de Seguridad de redes y servicios 5G.

Artículo 25. *Cooperación internacional.*

1. El Gobierno cooperará estrechamente con otros Estados miembros de la Unión Europea y con las instituciones de la Unión Europea en la definición y ejecución del Esquema Nacional de Seguridad de redes y servicios 5G y, en general, colaborará con las distintas organizaciones internacionales especializadas para poder llevar a cabo un tratamiento integral y global de la seguridad de las redes y servicios 5G.

2. En particular, el Gobierno y el Ministerio de Asuntos Económicos y Transformación Digital podrán compartir información relacionada con los análisis que realicen las instituciones de la Unión Europea y con otros Estados miembros de la Unión Europea preservando, como corresponda en Derecho, la seguridad, los intereses comerciales y la confidencialidad de la información recabada en la elaboración del análisis, así como servirse de la información que le envíen otros Estados o las instituciones de la Unión Europea para su realización. Igualmente, podrá llevar a cabo estos análisis de forma conjunta con otros Estados miembros de la Unión Europea.

Artículo 26. *Apoyo a la I+D+i en ciberseguridad 5G.*

El Esquema Nacional de Seguridad de redes y servicios 5G incluirá las líneas generales y prioridades de las ayudas públicas que pudieran ser convocadas para fomentar la investigación y el desarrollo en materia de seguridad en las redes y servicios 5G y para la formación de personal especializado.

Artículo 27. *Impulso a la interoperabilidad.*

El Esquema Nacional de Seguridad de redes y servicios 5G impulsará la interoperabilidad de los equipos y programas ligados a la gestión de redes y servicios 5G, así como la participación de actores públicos y privados en la elaboración de estándares sobre el funcionamiento de las redes y servicios 5G.

Artículo 28. *Facultades para la aplicación del Esquema Nacional de Seguridad de redes y servicios 5G.*

1. El Ministerio de Asuntos Económicos y Transformación Digital será el departamento competente para aplicar el Esquema Nacional de Seguridad de redes y servicios 5G y ejercer las demás funciones que le atribuye este real decreto-ley.

2. El Ministerio de Asuntos Económicos y Transformación Digital se coordinará con los demás órganos competentes en materia de ciberseguridad e infraestructuras críticas para garantizar una aplicación coherente del Esquema Nacional de Seguridad de redes y servicios 5G.

3. El Ministerio de Asuntos Económicos y Transformación Digital, en el ejercicio de las funciones que le asigna este real decreto-ley, podrá ejercer, entre otras, las siguientes facultades:

a) Desarrollar, concretar y detallar el contenido del Esquema Nacional de Seguridad de redes y servicios 5G.

b) Formular requerimientos de información a los sujetos previstos en el artículo 4, que deberán ser respondidos en el plazo de 15 días hábiles a contar desde el día siguiente al de su notificación, a efecto de poder ejercer las funciones que le asigna este real decreto-ley y su normativa de desarrollo y, en concreto, para verificar y controlar el cumplimiento de las respectivas obligaciones que este real decreto-ley y su normativa de desarrollo impone a los sujetos previstos en el artículo 4.

c) Realizar auditorías u ordenar su realización para verificar y controlar el cumplimiento de las respectivas obligaciones que este real decreto-ley y su normativa de desarrollo impone a los sujetos previstos en el artículo 4.

d) Realizar inspecciones por los funcionarios destinados en la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales y ejercer la potestad sancionadora en los términos indicados en el capítulo siguiente.

e) Conceder ayudas públicas.

f) Ejercer las demás funciones que le correspondan según la legislación aplicable.

CAPÍTULO V

Inspección y régimen sancionador

Artículo 29. *Facultades de inspección.*

El Ministerio de Asuntos Económicos y Transformación Digital ejercerá en la aplicación y supervisión de lo establecido en este real decreto-ley todas las potestades de la función inspectora previstas en el título VIII de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

Artículo 30. *Régimen sancionador.*

1. Será de aplicación el régimen sancionador establecido en el título VIII de la Ley 9/2014, de 9 de mayo, a excepción de las especialidades establecidas en este real decreto-ley.
2. Adicionalmente, se tipifican las siguientes infracciones clasificadas como muy graves, graves y leves.
3. Es infracción muy grave el incumplimiento por los operadores 5G que sean titulares o exploten elementos críticos de una red pública 5G de las obligaciones establecidas en el artículo 12.3.
4. Son infracciones graves:

a) El incumplimiento por los operadores 5G de las obligaciones establecidas en el artículo 12, excepto las contempladas en el artículo 12.3, que son infracciones calificadas como muy graves.
b) El incumplimiento por los suministradores 5G de las obligaciones establecidas en el artículo 13.
c) El incumplimiento por los usuarios corporativos 5G previstos en el artículo 4 de las obligaciones establecidas en el artículo 15.
d) El incumplimiento por las administraciones públicas de las obligaciones establecidas en el artículo 17.
e) El incumplimiento de estipulaciones establecidas en el Esquema Nacional de Seguridad de redes y servicios 5G cuando sean directamente exigibles.
f) El incumplimiento de los requerimientos de información formulados conforme al artículo 27.3.b) cuando haya pasado un mes desde la finalización del plazo dado para su cumplimiento.

5. Son infracciones leves los cumplimientos defectuosos o incumplimientos parciales de las conductas clasificadas como infracciones graves.
6. Las sanciones a aplicar son las establecidas en el artículo 79 de la Ley 9/2014, de 9 de mayo.
7. Los criterios para la determinación de la cuantía de la sanción son los establecidos en el artículo 80 de la Ley 9/2014, de 9 de mayo.
8. El ejercicio de la potestad sancionadora corresponde a la persona titular de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales.
9. Se podrán aplicar las medidas previas y las medidas cautelares establecidas en los artículos 81 y 82 de la Ley 9/2014, de 9 de mayo, cuando sea oportuno conforme a la regulación contenida en dichos artículos.

Artículo 31. *Inspección y régimen sancionador de la Ley General de Telecomunicaciones.*

En lo no previsto en este real decreto-ley, será de aplicación lo establecido en la regulación contenida en materia de inspección y régimen sancionador del título VIII de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

Disposición adicional primera. *Remisión al Ministerio de Asuntos Económicos y Transformación Digital de los análisis de riesgos de los operadores 5G y de las medidas técnicas y organizativas para mitigarlos.*

Los operadores 5G deberán remitir en el plazo de seis meses a contar desde la entrada en vigor de este real decreto-ley un análisis de riesgos de sus redes y servicios 5G o de los que vayan a desplegar en los próximos dos años y un informe de las medidas técnicas y organizativas diseñadas y aplicadas para gestionar y mitigar los riesgos.

Disposición adicional segunda. *Remisión al Ministerio de Asuntos Económicos y Transformación Digital de las estrategias de diversificación en la cadena de suministro.*

Los operadores 5G que sean titulares o exploten elementos críticos de una red pública 5G deberán remitir al Ministerio de Asuntos Económicos y Transformación Digital la estrategia de diversificación en la cadena de suministro en el plazo de seis meses a contar desde la entrada en vigor de este real decreto-ley.

Disposición adicional tercera. *Declaración de suministradores de alto riesgo.*

En el plazo de tres meses a contar desde la entrada en vigor de este real decreto-ley, el Gobierno, mediante acuerdo adoptado en Consejo de Ministros, previo informe del Consejo de Seguridad Nacional y previa audiencia de los operadores 5G y suministradores 5G afectados por un plazo de 15 días hábiles, podrá calificar que determinados suministradores 5G son de alto riesgo.

A tal efecto, el Gobierno analizará tanto las garantías técnicas de funcionamiento y operatividad de sus equipos, productos y servicios como su exposición a injerencias externas en los términos indicados en el artículo 14.

Disposición adicional cuarta. *Determinación de centros y ubicaciones en los que no se podrán utilizar equipos, productos o servicios de suministradores de alto riesgo.*

En el plazo de tres meses a contar desde la entrada en vigor de este real decreto-ley, el Consejo de Seguridad Nacional, previo informe del Ministerio de Asuntos Económicos y Transformación Digital, determinará las ubicaciones y centros en los que, en virtud de lo establecido en el artículo 12.3.c), por su vinculación a la seguridad nacional o al mantenimiento de determinados servicios esenciales para la comunidad o sectores estratégicos, los operadores 5G que sean titulares o exploten elementos críticos de una red pública 5G no podrán utilizar en la red de acceso de una red pública 5G equipos de telecomunicación, sistemas de transmisión, equipos de conmutación o encaminamiento y demás recursos, que permitan el transporte de señales, *hardware*, *software* o servicios auxiliares de suministradores de alto riesgo.

Disposición adicional quinta. *Aplicación del real decreto-ley a las sucesivas generaciones de comunicaciones electrónicas.*

Este real decreto-ley es de aplicación para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de generaciones posteriores a la quinta generación mientras no exista norma específica para las mismas.

Disposición transitoria única. *Sustitución de equipos, productos o servicios proporcionados por suministradores 5G declarados de alto riesgo.*

Si se produce la declaración de suministradores de alto riesgo en los términos indicados en la disposición adicional cuarta y ello trae como consecuencia que los operadores 5G tienen que sustituir los equipos, productos o servicios proporcionados por dichos suministradores 5G, los operadores 5G dispondrán de un plazo de cinco años a contar desde que los suministradores 5G hayan sido calificados de alto riesgo para llevar a cabo dicha sustitución en los elementos críticos de red relativos a las funciones del núcleo de la red y a los sistemas de control y gestión y los servicios de apoyo, así como de un plazo de dos años a contar desde que los suministradores 5G hayan sido calificados de alto riesgo para llevar a cabo dicha sustitución en los elementos críticos de red relativos a la red de

acceso en aquellas zonas geográficas y ubicaciones conforme a lo establecido en el artículo 12.3.c).

Disposición final primera. *Título competencial.*

Este real decreto-ley se dicta al amparo de lo previsto en el artículo 149.1.21.ª y en el artículo 149.1.29.ª de la Constitución, que atribuyen al Estado, respectivamente, competencia exclusiva en materia de régimen general de telecomunicaciones y en materia de seguridad pública.

Disposición final segunda. *Aplicación supletoria de la normativa sobre seguridad e integridad de las redes de comunicaciones electrónicas.*

1. En todo lo que no esté regulado en este real decreto-ley, será de aplicación supletoria lo dispuesto en la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, y su normativa de desarrollo.
2. En lo no regulado en la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, y su normativa de desarrollo, será aplicación supletoria el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, y la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, así como su respectiva normativa de desarrollo.

Disposición final tercera. *Habilitación para el desarrollo reglamentario.*

1. Se habilita al Gobierno para desarrollar reglamentariamente lo previsto en este real decreto-ley y, en particular, para aprobar el Esquema Nacional de Seguridad de redes y servicios 5G.
2. El primer Esquema Nacional de Seguridad de redes y servicios 5G deberá ser aprobado en el plazo de seis meses a contar desde la entrada en vigor de este real decreto-ley.

Disposición final cuarta. *Entrada en vigor.*

1. Este real decreto-ley entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».
2. Las obligaciones contenidas en los artículos, 12, 13, 15, 16 y 17 entrarán en vigor en el plazo de un mes a contar desde el día de su publicación en el «Boletín Oficial del Estado».

Información relacionada

- El Real Decreto-ley 7/2022, de 29 de marzo, ha sido convalidado por Acuerdo del Congreso de los Diputados, publicado por Resolución de 28 de abril de 2022. Ref. BOE-A-2022-7313

§ 46

Real Decreto 443/2024, de 30 de abril, por el que se aprueba el Esquema Nacional de Seguridad de redes y servicios 5G

Ministerio para la Transformación Digital y de la Función Pública
«BOE» núm. 106, de 1 de mayo de 2024
Última modificación: sin modificaciones
Referencia: BOE-A-2024-8715

Las comunicaciones móviles de quinta generación o 5G constituyen un nuevo paradigma de las comunicaciones electrónicas con un gran potencial transformador en beneficio de la sociedad y la economía, pues se abre la posibilidad a la incorporación de nuevas funcionalidades que van a tener un gran impacto, como la computación en la red y su virtualización y segmentación o sus funciones, lo que permitirá la creación de redes virtuales, flexibles e inteligentes, ofreciendo baja latencia, conectividad ininterrumpida y la prestación de servicios de gran valor añadido para la sociedad y la economía en ámbitos como la medicina, el transporte, la logística y la energía. Por todo ello, la Unión Europea y España, directamente y a través del Mecanismo de Recuperación y Resiliencia, impulsan el rápido despliegue de redes 5G y la realización de proyectos demostrativos de su utilidad para distintos sectores mediante la prestación de servicios 5G.

Pese a las ventajas que aportan, la utilización confiable de las redes y servicios 5G exige disponer de un elevado nivel de protección puesto que presentan riesgos específicos derivados, por ejemplo, de una arquitectura de red más compleja, basada en servicios y distribuida, con una banda ancha móvil mejorada, de mayor capacidad, para el transporte y transmisión de grandes volúmenes de datos a alta velocidad, fiabilidad y capacidad para conectar un número masivo de dispositivos a la red o la provisión de servicios específicos para determinados usos o aplicaciones. La naturaleza interconectada de su infraestructura, así como su carácter transnacional y la dimensión transfronteriza de las amenazas, comporta que cualquier vulnerabilidad o incidente de seguridad importante pueda tener implicaciones en funciones esenciales para la economía y la sociedad, llegando incluso a afectar a la Unión Europea en su conjunto.

Estos nuevos riesgos específicos de seguridad de las comunicaciones móviles 5G se abordaron regulatoriamente a través del Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación, que incorpora en toda su extensión la Recomendación (UE) 2019/534, de 26 de marzo de 2019, de la Comisión Europea, sobre la ciberseguridad de las redes 5G, el análisis coordinado de los Estados miembros y la «caja de herramientas», incluyéndose las recomendaciones de la Comunicación de 29 de enero de 2020 de la Comisión Europea «Despliegue seguro de la 5G en la UE-Aplicación de la caja de herramientas de la UE» (COM/2020/50 final).

El Real Decreto-ley 7/2022, de 29 de marzo, se ha visto modificado recientemente por la disposición final quinta del Real Decreto-ley 6/2023, de 19 de diciembre, por el que se

aprueban medidas urgentes para la ejecución del Plan de Recuperación, Transformación y Resiliencia en materia de servicio público de justicia, función pública, régimen local y mecenazgo, con el objetivo de reforzar los controles a efectuar por el Gobierno y el Ministerio para la Transformación Digital y de la Función Pública sobre las condiciones en las que se vienen efectuando la instalación de los distintos equipos, elementos, funciones y sistemas propios de la tecnología 5G, el despliegue de las redes 5G y la prestación de servicios de comunicaciones electrónicas 5G, en aras de alcanzar el objetivo último que persigue el Real Decreto-ley 7/2022, de 29 de marzo, que, como indica en su artículo 1, es el de establecer requisitos de seguridad para la instalación, el despliegue y la explotación de redes de comunicaciones electrónicas y la prestación de servicios de comunicaciones electrónicas e inalámbricas basados en la tecnología de quinta generación (5G).

La disposición final tercera del citado Real Decreto-ley 7/2022, de 29 de marzo, habilita al Gobierno para desarrollar reglamentariamente y aprobar el Esquema Nacional de Seguridad de redes y servicios 5G, lo que deberá realizarse mediante real decreto, a propuesta del Ministerio para la Transformación Digital y de la Función Pública, previo informe del Consejo de Seguridad Nacional, de acuerdo con el artículo 21 del Real Decreto-ley 7/2022, de 29 de marzo.

A su vez, los artículos 20 y 5.3 del Real Decreto-ley 7/2022, de 29 de marzo, establecen que el Esquema Nacional de Seguridad de redes y servicios 5G llevará a cabo un tratamiento integral y global de la seguridad de las redes y servicios 5G, considerando las aportaciones al alcance de cada agente de la cadena de valor de 5G para garantizar un funcionamiento continuado y seguro de la red y los servicios 5G, así como la normativa, las recomendaciones y los estándares técnicos de la Unión Europea, de la Unión Internacional de Telecomunicaciones (UIT) y de otras organizaciones internacionales, con el fin de garantizar el objetivo último de una explotación y operación seguras de las redes y servicios 5G en nuestro país. A tal efecto, en el Esquema Nacional de Seguridad de redes y servicios 5G se efectuará un análisis de riesgos a nivel nacional sobre la seguridad de las redes y servicios 5G y se identificarán, concretarán y desarrollarán medidas a nivel nacional para mitigar y gestionar los riesgos analizados.

En la búsqueda de este tratamiento integral de la seguridad de las redes y servicios 5G, el Esquema Nacional de Seguridad de redes y servicios 5G que se aprueba en este real decreto reconoce la existencia del Centro de Operaciones de Seguridad 5G de referencia, que depende del Ministerio para la Transformación Digital y de la Función Pública y que se encargará, entre otras tareas, de contribuir y apoyar al ejercicio de las facultades que al Ministerio para la Transformación Digital y de la Función Pública, y se le asignan en este ámbito funciones para proporcionar apoyo operativo a los sujetos obligados en actividades vinculadas a la prevención, protección, detección y respuesta frente a amenazas, incidentes y ciberataques a los sistemas, redes y servicios 5G, así como en la certificación y normalización de los mismos.

Para dar cumplimiento al mandato previsto en el artículo 21 y en la disposición final tercera del Real Decreto-ley 7/2022, de 29 de marzo, la presente norma aprueba el Esquema Nacional de Seguridad de las redes y servicios 5G.

Se cumple el principio de necesidad, pues este real decreto se dicta para garantizar un bien de interés general, como es la seguridad y confianza en las comunicaciones electrónicas. Es conforme con el principio de proporcionalidad ya que las medidas son adecuadas a los riesgos identificados en cada caso. Se ajusta al principio de seguridad jurídica porque se reconoce el marco normativo vigente en materia de seguridad y solo se añaden requisitos y controles adecuados a la singularidad de las redes y servicios 5G y sus riesgos. Se respeta el principio de transparencia, ya que los interesados han podido participar en el procedimiento de elaboración de la norma. Por último, cumple el principio de eficiencia pues se han limitado las cargas administrativas al mínimo imprescindible para conseguir el fin perseguido de garantizar la seguridad de las redes y servicios 5G.

Este real decreto ha sido sometido al procedimiento de información en materia de normas y reglamentaciones técnicas y de reglamentos relativos a los servicios de la sociedad de la información previsto en la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo, de 9 de septiembre de 2015, por la que se establece un procedimiento de

información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información.

Este real decreto se dicta al amparo de lo dispuesto en el artículo 149.1. 21.ª y en el artículo 149.1. 29.ª de la Constitución, que atribuyen al Estado, respectivamente, competencia exclusiva en materia de régimen general de telecomunicaciones y en materia de seguridad pública.

En la tramitación de este real decreto se ha emitido informe por el Consejo de Seguridad Nacional.

En su virtud, a propuesta del Ministro para la Transformación Digital y de la Función Pública, de acuerdo con el Consejo de Estado, y previa deliberación del Consejo de Ministros en su reunión del día 30 de abril de 2024,

DISPONGO:

Artículo único. *Aprobación del Esquema Nacional de Seguridad de las redes y servicios 5G.*

Se aprueba el Esquema Nacional de Seguridad de las redes y servicios 5G, que se inserta a continuación.

Disposición adicional primera. *Revisión del Esquema Nacional de Seguridad de las redes y servicios 5G.*

El Gobierno, mediante real decreto, a propuesta del Ministerio para la Transformación Digital y de la Función Pública, previo informe del Consejo de Seguridad Nacional, revisará el Esquema Nacional de Seguridad de redes y servicios 5G cuando las circunstancias lo aconsejen y, en todo caso, cada cuatro años.

Disposición adicional segunda. *Aplicación del Real Decreto-ley 7/2022, de 29 de marzo, y el Esquema Nacional de Seguridad de las redes y servicios 5G a las sucesivas generaciones de comunicaciones electrónicas.*

El Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación y el Esquema Nacional de Seguridad de las redes y servicios 5G que se aprueba, serán de aplicación a generaciones de comunicaciones electrónicas posteriores a la quinta generación mientras no exista norma específica para las mismas.

Disposición adicional tercera. *El Centro de Operaciones de Seguridad 5G de referencia en el marco del Plan de Recuperación, Transformación y Resiliencia.*

La creación del Centro de Operaciones de Seguridad 5G de referencia por el artículo 41 del Esquema Nacional de Seguridad de las redes y servicios 5G contribuye al cumplimiento de los hitos CID# 243 y 244 de la componente 15, inversión 6 (C15.I6) del Plan de Recuperación, Transformación y Resiliencia.

Disposición final primera. *Título competencial.*

Este real decreto y el esquema que aprueba se dictan al amparo de lo previsto en el artículo 149.1. 21.ª y en el artículo 149.1. 29.ª de la Constitución, que atribuyen al Estado, respectivamente, competencia exclusiva en materia de régimen general de telecomunicaciones y en materia de seguridad pública.

Disposición final segunda. *Aplicación supletoria de la normativa sobre seguridad e integridad de las redes de comunicaciones electrónicas.*

1. En todo lo que no esté regulado en este real decreto y el esquema que aprueba, será de aplicación supletoria lo dispuesto en la Ley 11/2022, de 28 de junio, General de Telecomunicaciones, y su normativa de desarrollo.

2. En lo no regulado en la Ley 11/2022, de 28 de junio, General de Telecomunicaciones, y su normativa de desarrollo, será aplicación supletoria el Real Decreto-ley 12/2018, de 7 de

septiembre, de seguridad de las redes y sistemas de información y la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, así como su respectiva normativa de desarrollo.

Disposición final tercera. *Habilitación para el desarrollo reglamentario y modificación de anexos.*

1. Se habilita a la persona titular del Ministerio para la Transformación Digital y de la Función Pública para desarrollar lo previsto en este real decreto y el esquema que aprueba, incluida la aprobación de instrucciones técnicas de seguridad.
2. Se habilita a la persona titular del Ministerio para la Transformación Digital y de la Función Pública para modificar mediante orden el contenido de los anexos del Esquema Nacional de Seguridad de las redes y servicios 5G en función de la evolución del avance tecnológico, de la aprobación de nuevos estándares técnicos y esquemas de certificación de equipos de telecomunicación y productos conectados y del desarrollo de diferentes configuraciones y parámetros técnicos de redes y servicios 5G y de venideras generaciones de comunicaciones electrónicas.

Disposición final cuarta. *Entrada en vigor.*

Este real decreto y el esquema que aprueba entrarán en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

ESQUEMA NACIONAL DE SEGURIDAD DE LAS REDES Y SERVICIOS 5G

CAPÍTULO I

Disposiciones generales

Artículo 1. *Esquema Nacional de Seguridad de las redes y servicios 5G.*

El Esquema Nacional de Seguridad de las redes y servicios 5G (en adelante, ENS5G) se aprueba en desarrollo de lo establecido en el Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación, en particular, en aplicación de su capítulo IV.

Artículo 2. *Objetivos.*

El ENS5G tiene los siguientes objetivos:

a) Reforzar la protección de la seguridad nacional.
b) Garantizar un funcionamiento continuado y seguro de las redes y servicios 5G.
c) Llevar a cabo un tratamiento integral y global de la seguridad de las redes y servicios 5G, considerando las aportaciones al alcance de cada agente de la cadena de valor de 5G.
d) Reforzar la seguridad en la instalación y operación de las redes de comunicaciones electrónicas 5G y en la prestación de los servicios de comunicaciones móviles e inalámbricas que se apoyen en las redes 5G.
e) Impulsar una seguridad integral del ecosistema generado por la tecnología 5G.
f) Promover un mercado de suministradores en las redes y servicios de comunicaciones electrónicas 5G suficientemente diversificado en aras de garantizar la seguridad basada en razones técnicas, estratégicas y operativas y evitar, por dichas razones, la presencia de suministradores con una calificación de alto riesgo o de riesgo medio en determinados elementos de red o ámbitos.
g) Fortalecer la industria y fomentar las actividades de I+D+i nacionales en ciberseguridad relacionadas con la tecnología 5G.
h) Impulsar la formación y la concienciación en ciberseguridad 5G.

Artículo 3. *Definiciones.*

A los efectos del ENS5G, se utilizarán las definiciones establecidas en el Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación, así como las definiciones establecidas en la Ley 11/2022, de 28 de junio, General de Telecomunicaciones, y en la Directiva 2018/1972, de 11 de diciembre de 2018, del Parlamento Europeo y del Consejo, por la que se establece el Código Europeo de las Comunicaciones Electrónicas.

El concepto de Seguridad Integral recogido en el ENS5G, se refiere a que la seguridad se entiende como un proceso integral constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos, dentro del ámbito y el marco de la seguridad de las redes y servicios 5G regulada por el Real Decreto-ley 7/2022, de 29 de marzo.

Artículo 4. *Ámbito de aplicación.*

1. El ENS5G, en el marco de la seguridad de redes y servicios 5G regulada en el Real Decreto-ley 7/2022, de 29 de marzo, se aplica a los siguientes sujetos obligados:

a) Operadores 5G, definidos en el artículo 3.1, apartado a) del Real Decreto-ley 7/2022, de 29 de marzo.

b) Suministradores 5G, definidos en el artículo 3.1, apartado f) del Real Decreto-ley 7/2022, de 29 de marzo.

c) Usuarios corporativos 5G que tengan otorgados derechos de uso del dominio público radioeléctrico para instalar, desplegar o explotar una red privada 5G o prestar servicios 5G para fines profesionales o en autoprestación, definidos en el artículo 3.1, apartado g) del Real Decreto-ley 7/2022, de 29 de marzo.

2. El ENS5G también se aplica a las entidades de las Administraciones públicas que instalen, desplieguen y exploten redes 5G, ya sean públicas o privadas, o presten servicios 5G, disponibles al público o en autoprestación, cuando sus actividades no se lleven a cabo principalmente en los ámbitos de la seguridad nacional, la seguridad pública, la defensa nacional o la garantía del cumplimiento de la ley, incluidas la prevención, investigación, detección y enjuiciamiento de infracciones penales. Adicionalmente por su carácter excepcional, no se aplica en el ámbito de la defensa nacional a nivel general y, en particular, en las actividades de preparación y participación en operaciones militares por parte de las Fuerzas Armadas.

Artículo 5. *Red 5G.*

1. Una red de comunicaciones electrónicas 5G está integrada, al menos, por los siguientes elementos, infraestructuras y recursos:

a) Los relativos a las funciones del núcleo de la red.

b) Las funciones de transporte y transmisión.

c) La red de acceso.

d) Los sistemas de control y gestión y los servicios de apoyo.

e) Las funciones de computación en el borde, virtualización de red y gestión de sus componentes.

f) Los relativos a intercambios de tráfico o interconexión con redes externas e Internet.

g) Otros componentes y funciones a los que se refiere el anexo I.

2. Forman parte de la red 5G la totalidad de los elementos de red, infraestructuras, recursos y funciones de las redes empleadas para ofrecer servicios 5G, aun cuando también sean usados en las redes y servicios de comunicaciones electrónicas de generaciones móviles precedentes, de acuerdo con el artículo 3.1, apartado b) del Real Decreto-ley 7/2022, de 29 de marzo.

3. La descripción detallada de los elementos, infraestructuras y recursos que integran una red 5G figura en el anexo I.

4. Dentro de cada una de las partes o elementos de una red 5G, sean partes o elementos críticos o no de la red 5G en los términos indicados en el artículo 6, apartados 2 y 3, del Real Decreto-ley 7/2022, de 29 de marzo, y en este artículo y en el siguiente, existirán

diferentes activos que pueden presentar diferente grado de criticidad (alta, media, baja) en el análisis de riesgos en los términos indicados en el anexo II.

Artículo 6. *Elementos críticos de una red 5G.*

1. Son elementos críticos de una red 5G:

a) Los relativos a las funciones del núcleo de la red.
b) Los sistemas de control y gestión y los servicios de apoyo.
c) La red de acceso en aquellas zonas geográficas y ubicaciones que se determine.

2. Los elementos críticos de una red 5G pública deberán ubicarse dentro del territorio nacional, de acuerdo con el artículo 12.3, apartado e), del Real Decreto-ley 7/2022, de 29 de marzo.

3. No obstante, determinados elementos, funciones y sistemas tanto del núcleo de la red como de los sistemas de control y gestión y los servicios de apoyo podrán ubicarse fuera del territorio nacional, siempre y cuando el Ministerio para la Transformación Digital y de la Función Pública pueda ejercer las facultades que le atribuye el Real Decreto-ley 7/2022, de 29 de marzo, en particular, las facultades de inspección y régimen sancionador previstas en su capítulo V, de manera que pueda efectuar una verificación integral sobre el funcionamiento, operatividad y condiciones de uso de dichos elementos críticos de una red 5G y, en su caso, poder adoptar medidas, cautelares o definitivas, sobre dichos elementos, funciones y sistemas o el equipamiento utilizado en el ejercicio de las potestades que al Ministerio para la Transformación Digital y de la Función Pública le atribuye el Real Decreto-ley 7/2022, de 29 de marzo y la Ley 11/2022, de 28 de junio, General de Telecomunicaciones.

4. En el caso de que el Consejo de Ministros, previo informe del Ministerio para la Transformación Digital y de la Función Pública, llegue a la conclusión de que los elementos, funciones y sistemas tanto del núcleo de la red como de los sistemas de control y gestión y los servicios de apoyo que estén ubicados fuera del territorio nacional afecten a la seguridad o integridad de la red 5G teniendo en cuenta el análisis de las medidas técnicas o las medidas estratégicas relacionadas en los artículos 15.2 y 15.3, respectivamente, o condiciona sensiblemente el ejercicio de sus facultades de supervisión y potestades de inspección, podrá requerir al titular de la red 5G que dichos elementos, funciones y sistemas se ubiquen en territorio nacional. A tal efecto, la reubicación de los elementos, funciones y sistemas deberá producirse en el plazo que indique el Consejo de Ministros en su acuerdo, a propuesta del Ministerio para la Transformación Digital y de la Función Pública, previa audiencia del titular de la red 5G, si bien este plazo no podrá ser inferior a un año.

Artículo 7. *Tratamiento integral de la seguridad.*

1. La seguridad se entiende como un proceso integral constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con las redes o servicios 5G de los sujetos obligados afectados por el ámbito de aplicación y debe incorporarse desde el diseño e implementación de las redes 5G. El ENS5G tiene la vocación de llevar a cabo un tratamiento integral de la seguridad de las redes y servicios 5G.

2. A tal efecto, el ENS5G ha tenido en cuenta y deberá tener en cuenta en futuras actualizaciones o modificaciones la normativa, las recomendaciones y los estándares técnicos de la Unión Europea, de la Unión Internacional de Telecomunicaciones (UIT) y de otras organizaciones internacionales.

Asimismo, el ENS5G ha tenido en cuenta y deberá tener en cuenta en futuras actualizaciones o modificaciones las aportaciones, análisis de riesgos, planes de mitigación de riesgos y estrategias de diversificación de la cadena de suministro que se han ido proporcionando y que deberán proporcionar por los sujetos obligados en cumplimiento de las obligaciones establecidas en el Real Decreto-ley 7/2022, de 29 de marzo, en este esquema y en el resto de normativa.

3. En este contexto de seguridad integral, los sujetos obligados deberán llevar a cabo un tratamiento integral y global de la seguridad de las redes, elementos, infraestructuras, recursos, facilidades y servicios de los que sean responsables, para lo cual deberán realizar, mediante un método holístico, un análisis de las vulnerabilidades, amenazas y riesgos que

les afecten como agentes económicos y de los componentes anteriormente relacionados, así como una gestión adecuada e integral de dichos riesgos mediante la utilización de las técnicas y medidas que sean adecuadas para lograr su mitigación o eliminación y alcanzar el objetivo final de una explotación y operación seguras de las redes y servicios 5G, considerando también las aportaciones de cada agente de la cadena de valor de 5G.

4. A fin de llevar a cabo un tratamiento integral de la seguridad de las redes y servicios 5G, el operador 5G deberá recabar de sus suministradores 5G las prácticas y medidas de seguridad que hubieren adoptado en los productos y servicios suministrados. Esta información deberá ser proporcionada por los suministradores 5G y su tratamiento será confidencial, de manera que sólo podrá ser utilizada por los operadores 5G para efectuar un análisis y gestión de riesgos y por el Ministerio para la Transformación Digital y de la Función Pública y los demás organismos públicos competentes para la aplicación de lo dispuesto en el Real Decreto-ley 7/2022, de 29 de marzo y este esquema.

5. Los sujetos obligados podrán enviar al Centro de Operaciones de Seguridad 5G de referencia a que se refiere el artículo 41 los datos requeridos para la detección del estado de la ciberseguridad de las redes y servicios 5G en tiempo real.

6. El Ministerio para la Transformación Digital y de la Función Pública, directamente o a través del Centro de Operaciones de Seguridad 5G de referencia a que se refiere el artículo 41, podrá formular los requerimientos de información necesarios a los sujetos obligados, que deberán ser respondidos en el plazo de 15 días hábiles a contar desde el día siguiente al de su notificación, a efecto de poder ejercer las funciones que le asigna el Real Decreto-ley 7/2022, de 29 de marzo.

Artículo 8. *Gestión de la seguridad basada en los riesgos.*

1. El análisis y la gestión de los riesgos es parte esencial del proceso de seguridad, debiendo constituir una actividad continua y permanentemente actualizada.

2. La gestión de riesgos permitirá el mantenimiento de un entorno controlado en la red o servicio 5G, minimizando los riesgos a niveles aceptables. La reducción a estos niveles se realizará mediante una apropiada aplicación de medidas de seguridad, de manera equilibrada y proporcionada a la naturaleza y características de la red, de los servicios a prestar y de los riesgos a los que estén expuestos, que deberán reflejarse en el análisis de riesgos.

Artículo 9. *Prevención, detección, respuesta y conservación.*

1. La seguridad de los sistemas, redes y servicios 5G debe contemplar las acciones relativas a los aspectos de prevención, detección y respuesta, al objeto de minimizar sus vulnerabilidades y lograr que las amenazas no se materialicen o que, en el caso de hacerlo, no afecten gravemente a los datos tratados, a la operatividad e integridad de las redes 5G o a la prestación de un servicio 5G.

2. Las medidas de prevención, para ampliar el conocimiento de las vulnerabilidades, que podrán incorporar componentes orientados a la disuasión o a la reducción de la superficie de exposición, deben eliminar o reducir la probabilidad de que las amenazas lleguen a materializarse.

3. Las medidas de detección irán dirigidas a descubrir la presencia de un ciberincidente, una ciberamenaza o vulnerabilidad.

4. Las medidas de respuesta, orientadas a minimizar el impacto de los ciberincidentes y, en su caso, aplicando medidas de bloqueo, así como posteriormente la restauración del sistema, red o servicio 5G que pudiera haberse visto afectado por un incidente de seguridad.

5. Sin merma de los restantes principios básicos y requisitos mínimos establecidos, el sistema de información garantizará la conservación de los datos e información en soporte electrónico.

Artículo 10. *Existencia de líneas de defensa.*

1. Las redes, elementos, infraestructuras, recursos, facilidades y servicios 5G han de disponer de una estrategia de protección y diversificación adecuada y proporcionada a los

riesgos de cada elemento y capa de servicios 5G, de tal forma que, cuando uno de ellos se pueda ver comprometida, dicha estrategia permita:

a) Una reacción adecuada frente a los incidentes que no han podido evitarse, reduciendo la probabilidad de que el sistema sea comprometido en su conjunto.
b) Minimizar el impacto final del incidente.

2. La estrategia de protección y las líneas de defensa estarán constituidas por medidas de naturaleza organizativa, física y lógica. Se determinarán en las correspondientes instrucciones técnicas de seguridad.

Artículo 11. *Vigilancia continua y reevaluación periódica.*

1. La vigilancia continua permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta.
2. La evaluación permanente del estado de la seguridad de las redes y servicios 5G permitirán medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.
3. Las medidas de seguridad se reevaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.

Artículo 12. *Sistemas, redes y servicios 5G que traten datos personales.*

Cuando un sistema, red o servicio 5G trate datos personales le será de aplicación lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecto al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos) y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, o en su caso, el resto de normativa de aplicación, así como los criterios que se establezcan por la Agencia Española de Protección de Datos o en su ámbito competencial, por las autoridades autonómicas de protección de datos, sin perjuicio de los requisitos establecidos en el presente real decreto.

CAPÍTULO II

Análisis y gestión de riesgos a nivel nacional

Artículo 13. *Análisis de riesgos a nivel nacional.*

1. El análisis de riesgos a nivel nacional que se ha realizado en el marco del ENS5G es el que figura en el anexo II de este real decreto.
2. En la realización de este análisis, se ha tenido en cuenta:

a) El análisis general de los riesgos de las redes y servicios 5G, tomando en consideración la información recabada de los sujetos obligados.
b) El examen de las vulnerabilidades ligadas a la cadena de suministro de las redes y servicios 5G.
c) La evaluación del grado de dependencia de los suministradores del conjunto de las redes y servicios 5G en España teniendo en cuenta los análisis de riesgos y las estrategias de diversificación de suministradores remitidos por los operadores 5G, así como el riesgo de interrupción del suministro por circunstancias económicas, societarias o comerciales que afecten a los suministradores.
d) La evaluación de la eficacia de las medidas de seguridad aplicadas hasta la aprobación de cada análisis de riesgos nacional para mitigar los riesgos puestos de manifiesto por tal análisis.
e) La determinación de una jerarquía de riesgos en función de los análisis de riesgos llevados a cabo por los sujetos obligados.

Artículo 14. *Gestión de riesgos a nivel nacional.*

1. Los criterios, requisitos, condiciones y plazos para que los sujetos obligados puedan diseñar e implementar técnicas y medidas de mitigación de riesgos son los que, al menos, figuran en el anexo III de este real decreto.

2. En la determinación de estos criterios y requisitos de gestión de riesgos se han tenido en cuenta el análisis de riesgos nacional que incorpora este esquema y la evaluación de la eficacia de las medidas aplicadas por los sujetos obligados para mitigar y gestionar los riesgos en las redes y servicios 5G.

CAPÍTULO III

Medidas específicas para garantizar la seguridad de las redes y servicios 5G

Artículo 15. *Declaración de suministradores 5G de alto riesgo y de riesgo medio.*

1. El Gobierno, mediante acuerdo adoptado en Consejo de Ministros, podrá calificar que determinados suministradores 5G son de alto riesgo.

A tal efecto, el Gobierno analizará tanto las garantías técnicas de funcionamiento y operatividad de sus equipos, productos y servicios como su exposición a injerencias externas.

2. En relación con el análisis de las medidas y las garantías técnicas de funcionamiento y operatividad de sus equipos, productos y servicios se valorarán aspectos relativos al cumplimiento de normas o especificaciones técnicas, su verificación mediante esquemas de certificación, o la superación de pruebas o auditorías de seguridad realizadas por entidades independientes.

3. En relación con el análisis de las medidas estratégicas y exposición a injerencias externas, se valorarán los siguientes aspectos:

a) Los vínculos de los suministradores y de su cadena de suministro, con los gobiernos de terceros países.

b) La composición de su capital social y la estructura de sus órganos de gobierno.

c) El poder de un tercer Estado para ejercer presión sobre la actuación o ubicación de la empresa.

d) Las características de la legislación y la política de ciberdefensa y el respeto al derecho internacional y a las resoluciones y acuerdos de la Organización de las Naciones Unidas de ese tercer Estado.

e) Los acuerdos de cooperación en materia de seguridad, ciberseguridad, delitos cibernéticos o protección de datos firmados con el país tercero de que se trate, así como los tratados internacionales en esas materias de que sea parte dicho Estado.

f) El grado de adecuación de la normativa del tercer Estado sobre protección de datos personales a la de España, al Reglamento General de Protección de Datos aprobado por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, adoptada por la Unión Europea y a cualquier otra normativa aplicable en materia de seguridad de las redes y sistemas de información y de telecomunicaciones.

4. El procedimiento para la calificación de determinados suministradores 5G como de alto riesgo se iniciará de oficio mediante acuerdo adoptado por el Ministerio para la Transformación Digital y de la Función Pública.

En la tramitación del expediente se solicitará informe a la Comisión Nacional de los Mercados y la Competencia, al Ministerio del Interior, al Ministerio de Defensa, al Departamento de Seguridad Nacional del Gabinete de la Presidencia del Gobierno, al Centro Nacional de Inteligencia del Ministerio de Defensa y al Instituto Nacional de Ciberseguridad de España.

En la propuesta de resolución, el Ministerio para la Transformación Digital y de la Función Pública concretará en relación con el suministrador 5G afectado las garantías técnicas de funcionamiento y operatividad de los equipos, productos y servicios suministrados así como su exposición a injerencias externas conforme a lo indicado en los

apartados anteriores que justifican la decisión propuesta, así como las consecuencias que de dicha decisión se derivan y, en caso de que se declare suministrador de alto riesgo, el plazo en que los operadores 5G deberán llevar a cabo la sustitución de los equipos, productos y servicios proporcionados por dicho suministrador.

De la propuesta de resolución se dará audiencia a los operadores 5G y suministradores 5G afectados por un plazo de 15 días hábiles.

Una vez efectuados estos trámites, el Gobierno, mediante acuerdo adoptado en Consejo de Ministros, previo informe del Consejo de Seguridad Nacional, adoptará una decisión en el plazo de seis meses a contar desde la incoación del procedimiento.

5. El acuerdo del Consejo de Ministros por el que se califique a determinados suministradores 5G como suministradores de alto riesgo determinará el plazo en que los operadores 5G deberán llevar a cabo la sustitución de los equipos, productos y servicios proporcionados por dicho suministrador en la red y servicios del operador 5G, cuando ello fuera necesario, para lo cual deberá tener en cuenta las amenazas detectadas y los motivos que han justificado la declaración de un suministrador 5G como suministrador de alto riesgo, la situación del mercado de los suministradores, las alternativas de suministro de equipos y productos sustitutivos viables, la implantación de esos equipos y productos en la red 5G del operador, especialmente en los elementos críticos de la red 5G y en función de cuáles son en concreto los elementos críticos afectados, la dificultad intrínseca para llevar a cabo la sustitución de equipos, los ciclos de actualización de equipos, la migración de las redes 5G no autónomas a autónomas, así como su impacto económico.

En la determinación del plazo de sustitución, el acuerdo del Consejo de Ministros por el que se califique a determinados suministradores 5G como suministradores de alto riesgo podrá establecer un plazo diferente para los distintos elementos críticos de la red pública 5G en función de las amenazas detectadas y los motivos que han justificado la declaración de un suministrador 5G como suministrador de alto riesgo, la criticidad de dicho elemento o parte de él, de su afectación al funcionamiento y operatividad de la red y de la disponibilidad de equipos en ese momento en el mercado de equipos de telecomunicación, si bien, en ningún caso, este plazo podrá ser inferior a un año para cualquier elemento crítico de la red pública 5G.

El acuerdo del Consejo de Ministros por el que se califique a determinados suministradores 5G como suministradores de alto riesgo podrá determinar un plazo diferente para la sustitución de los equipos, productos y servicios para los distintos operadores 5G afectados en función de la repercusión que dicha sustitución tiene en la red de cada operador, de la afectación de la sustitución a los distintos elementos o partes de la red 5G, de la capacidad competitiva del operador, de los contratos de suministro de equipamiento suscritos y de la capacidad de suministro existente en el mercado de equipos de telecomunicación, si bien, en ningún caso, ese plazo podrá ser inferior a un año para cualquier elemento crítico de la red pública 5G.

6. El acuerdo del Consejo de Ministros por el que se califique que determinados suministradores 5G son de alto riesgo pone fin a la vía administrativa y es directamente recurrible ante la jurisdicción contencioso-administrativa, sin perjuicio de que potestativamente se pueda interponer contra el mismo un recurso de reposición con carácter previo al recurso contencioso-administrativo.

7. Los suministradores de alto riesgo cuyos equipos de telecomunicación, hardware, software o servicios auxiliares proporcionados sean utilizados única y exclusivamente en redes privadas 5G o para la prestación de servicios 5G en régimen de autoprestación son calificados como suministradores de riesgo medio.

Artículo 16. *Determinación de ubicaciones en las que no se podrá instalar equipos de suministradores calificados de alto riesgo.*

1. El Consejo de Seguridad Nacional, previo informe del Ministerio para la Transformación Digital y de la Función Pública, podrá determinar las ubicaciones, áreas y centros en las que no se podrá instalar equipos de suministradores calificados de alto riesgo. En la emisión de su informe, el Ministerio para la Transformación Digital y de la Función Pública tendrá en cuenta las propuestas que le remitan el Ministerio del Interior, el Ministerio

de Defensa, el Departamento de Seguridad Nacional del Gabinete de la Presidencia del Gobierno y el Centro Nacional de Inteligencia del Ministerio de Defensa.

2. En la determinación de estas ubicaciones, áreas y centros se incluirán las centrales nucleares, centros vinculados a la Defensa Nacional y las ubicaciones, áreas y centros que, por su vinculación a la seguridad nacional o al mantenimiento de determinados servicios esenciales para la comunidad o sectores estratégicos, sean determinados por Consejo de Seguridad Nacional.

3. En las estaciones radioeléctricas con las que se proporcione cobertura a estas ubicaciones, áreas y centros, los operadores 5G no podrán utilizar en la red de acceso radio de una red pública 5G equipos de telecomunicación, sistemas de transmisión, equipos de conmutación o encaminamiento y demás recursos, que permitan el transporte de señales, hardware, software o servicios auxiliares de suministradores que hayan sido calificados de alto riesgo.

4. Asimismo, para la instalación, modificación o adaptación de estaciones radioeléctricas que proporcionen cobertura a estas ubicaciones, áreas y centros previamente declarados, habida cuenta de su vinculación con la seguridad nacional o al mantenimiento de determinados servicios esenciales para la comunidad o sectores estratégicos, los operadores 5G deberán solicitar autorización a la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, en cuyo otorgamiento se tendrán en cuenta los equipos de telecomunicación, sistemas de transmisión, equipos de conmutación o encaminamiento y demás recursos, que permitan el transporte de señales, hardware, software o servicios auxiliares a instalar, las condiciones técnicas en el uso del dominio público radioeléctrico y las características intrínsecas y fines a proteger en esas ubicaciones, áreas y centros previamente declarados.

La Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, en el otorgamiento de estas autorizaciones, podrá valorar los planes que los operadores 5G puedan presentar para la renovación tecnológica o la sustitución de equipos de transmisión radio y en la red de acceso que afecten a las ubicaciones, áreas y centros previamente declarados para las que se solicita autorización.

El plazo para el otorgamiento de estas autorizaciones es de tres meses, entendiéndose desestimada la solicitud en caso de ausencia de resolución expresa. La resolución, expresa o presunta, pone fin a la vía administrativa y es directamente recurrible ante la jurisdicción contencioso-administrativa, sin perjuicio de que potestativamente se pueda interponer contra el mismo un recurso de reposición con carácter previo al recurso contencioso-administrativo.

Queda exceptuado de la necesidad de obtener la autorización a que se refiere este apartado las operaciones de ampliación, adaptación, reparación y mantenimiento de estaciones radioeléctricas que proporcionen cobertura a estas ubicaciones, áreas y centros siempre y cuando dicha estación ya esté previamente instalada y autorizada y no implique ningún cambio de suministrador en ninguno de los elementos, hardware, software o capas en los sistemas que configuran la estación.

Quedan exceptuados de la solicitud de autorización la ampliación del equipamiento radioeléctrico ubicado en un nodo de un mismo suministrador por razones de capacidad, que ya se encuentre previamente instalado y autorizado conforme a los párrafos anteriores, así como cualquier operación de mantenimiento y reparación.

5. Las obligaciones establecidas en los apartados 3 y 4 de este artículo se aplican de forma exclusiva a los elementos de la red de acceso radio 5G según la definición del 3GPP mencionada en el anexo I.

6. La determinación y difusión de estas ubicaciones tendrán la calificación de materia reservada conforme a la regulación establecida en la Ley 9/1968, de 5 de abril, sobre secretos oficiales.

Artículo 17. *Diversificación en la cadena de suministro.*

1. De acuerdo con lo previsto en el artículo 12.3.a) del Real Decreto-ley 7/2022, de 29 de marzo, los operadores 5G que sean titulares o exploten elementos críticos de una red pública 5G deberán diseñar una estrategia de diversificación en la cadena de suministro de los equipos de telecomunicación, sistemas de transmisión, equipos de conmutación o

encaminamiento y demás recursos que permitan el transporte de señales en una red pública 5G.

2. En la red de acceso, los operadores 5G deberán contar con equipos de transmisión radio que sean proporcionados, como mínimo, por dos suministradores diferentes a efecto de favorecer la continuidad de los servicios 5G, la más fácil sustituibilidad de los equipos y evitar la dependencia exclusiva de un suministrador único.

A estos efectos, se considera que los suministradores no son diferentes si todos ellos pertenecen al mismo grupo de empresas, conforme a los criterios establecidos en el artículo 42 del Código de Comercio.

3. En el núcleo de la red y en los sistemas de control y gestión y los servicios de apoyo, el suministrador podrá ser único.

4. En el caso de que como consecuencia de operaciones de concentración empresarial, se redujera el número de suministradores incluidos en la estrategia de diversificación en la cadena de suministro que implicara que no se cumpliera el límite mínimo de dos suministradores diferentes establecido en el apartado 2, el operador 5G deberá comunicárselo al Ministerio para la Transformación Digital y de la Función Pública, que impulsará que el Gobierno, mediante acuerdo adoptado en Consejo de Ministros, previa audiencia de los operadores 5G y suministradores 5G afectados, decida si resulta posible mantener un suministrador único, teniendo en cuenta las condiciones concretas de la operación de concentración empresarial, la situación del mercado de los suministradores, las alternativas de suministro de equipos y productos sustitutivos viables, la implantación de esos equipos y productos en la red 5G del operador, especialmente en los elementos críticos de la red 5G, la calificación del suministrador como de alto riesgo, la dificultad intrínseca para llevar a cabo la sustitución de equipos, los ciclos de actualización de equipos, la migración de las redes 5G no autónomas a autónomas, así como su impacto económico.

5. El Ministerio para la Transformación Digital y de la Función Pública, si considera que no queda garantizada la continuidad en la prestación de los servicios 5G, la integridad física o lógica de la red 5G, que existe una amplia exposición al equipamiento instalado por un suministrador que en determinadas circunstancias puede poner en peligro la funcionalidad y operatividad de la red 5G o para garantizar la seguridad en la provisión de servicios utilizados por los servicios de Seguridad Nacional, Defensa Nacional o por distintas Administraciones Públicas, y teniendo en cuenta si existe calificación de suministradores de alto riesgo, las alternativas de suministro de equipos y productos sustitutivos viables, la implantación de esos equipos y productos en la red 5G del operador, especialmente en los elementos críticos de la red 5G, y los ciclos de actualización de equipos, podrá modificar la estrategia de diversificación en la cadena de suministro de un operador 5G.

Antes de aprobar la modificación, se deberá efectuar un trámite de audiencia con el operador 5G y suministrador o suministradores 5G afectados por un plazo de 15 días hábiles. La resolución pone fin a la vía administrativa y es directamente recurrible ante la jurisdicción contencioso-administrativa, sin perjuicio de que potestativamente se pueda interponer contra la misma un recurso de reposición con carácter previo al recurso contencioso-administrativo.

CAPÍTULO IV

Análisis de riesgos por los sujetos obligados

Artículo 18. *Análisis de riesgos por los operadores 5G.*

1. Los operadores 5G deberán analizar los riesgos de las redes y servicios 5G, detectando vulnerabilidades y amenazas que les afecten, tanto como agente económico, como por los elementos de red, infraestructuras, recursos, facilidades y servicios que empleen o provean en la instalación, despliegue y explotación de redes 5G o en la prestación de servicios 5G.

2. Los operadores 5G que sean titulares o gestionen elementos de red de una red pública 5G, en su análisis de riesgos, deberán llevar a cabo un estudio pormenorizado e individualizado de las amenazas y vulnerabilidades que afecten a los elementos,

infraestructuras y recursos que integran una red 5G y que figuran en el anexo I, siguiendo la metodología descrita en el anexo II, apartado 1.

3. El análisis de riesgos que lleve a cabo un operador 5G deberá tener en cuenta, al menos, los siguientes factores:

a) Parametrización y configuración de elementos y funciones de red, incluidos los equipos de telecomunicación, hardware y software y servicios auxiliares que intervengan en el funcionamiento u operación de redes 5G o en la prestación de servicios 5G.

b) Políticas de integridad y actualización de los programas informáticos para garantizar la seguridad y funcionalidad de la red en todo momento.

c) Estrategias de permisos de acceso a activos físicos y lógicos, garantizando que sólo el personal autorizado pueda acceder a recursos críticos.

d) Evaluación de las dependencias de determinados proveedores en elementos críticos de la red 5G, identificando riesgos potenciales asociados con la cadena de suministro.

e) Identificación y evaluación de amenazas potenciales de agentes externos, incluyendo grupos organizados con capacidad para atacar la red.

f) Consideración de los equipos terminales y dispositivos conectados a la red, y su impacto en la seguridad global de la red.

g) Análisis de la interacción y el impacto de la red 5G sobre elementos de usuarios corporativos y redes externas conectadas.

h) Comprensión de la interrelación de la red 5G con otros servicios esenciales para la sociedad, evaluando cómo posibles interrupciones del servicio o compromisos de seguridad pueden afectar a estos servicios esenciales.

i) Priorización y jerarquización de riesgos basados en la afectación a elementos críticos de la red, el tipo de recurso, infraestructura y servicio afectado, la integridad y mantenimiento técnico de la red, la capacidad de detección y recuperación, el número y tipo de usuarios afectados, y el tipo de información comprometida.

j) Implementación de estrategias de resiliencia y recuperación ante desastres, para asegurar la continuidad del servicio frente a ataques cibernéticos, incidencias técnicas o desastres naturales, incluyendo la redundancia de sistemas críticos.

k) Realización de análisis de vulnerabilidades de manera regular, para identificar proactivamente vulnerabilidades de seguridad y resolverlas para mitigar posibles amenazas antes de que puedan ser explotadas.

4. A fin de llevar a cabo un tratamiento integral de la seguridad de las redes y servicios 5G, el suministrador deberá proporcionar a los operadores 5G a los que suministre las prácticas y medidas de seguridad que se han adoptado en los productos y servicios que han suministrado, teniendo en cuenta los factores de riesgo indicados en este capítulo y el perfil de riesgo del suministrador. Esta información deberá ser recibida por los operadores 5G y su tratamiento será confidencial, de manera que sólo podrá ser utilizada por los operadores 5G para efectuar un análisis y gestión de riesgos y por el Ministerio para la Transformación Digital y de la Función Pública y los demás organismos públicos competentes para la aplicación de lo dispuesto en el Real Decreto-ley 7/2022, de 29 de marzo y en este esquema a los exclusivos fines de los mismos.

5. El análisis de riesgos del operador 5G deberá incluir una priorización y jerarquía de los riesgos en función de los siguientes parámetros:

a) Afectación a un elemento crítico de la red pública 5G.

b) Tipo de recurso, infraestructura y servicio que pueda verse afectado.

c) Afectación a la integridad y mantenimiento técnico de la red o a la continuidad del servicio.

d) Capacidad de detección y recuperación.

e) Número y tipo de usuarios afectados.

f) Tipo de información cuya integridad haya podido verse comprometida.

6. Un nuevo análisis de riesgos por el operador 5G debe ser llevado a cabo y ser remitido al Ministerio para la Transformación Digital y de la Función Pública antes del 1 de octubre de 2024, y, a continuación, cada dos años o cuando le sea requerido para ello por el Ministerio para la Transformación Digital y de la Función Pública siempre que se hayan

producido cambios significativos en las infraestructuras 5G utilizadas o servicios 5G prestados que induzcan a pensar que las medidas de seguridad adoptadas pudieran haber perdido eficacia.

Artículo 19. *Análisis de riesgos por los suministradores 5G.*

1. Los suministradores 5G deben analizar los riesgos de los equipos de telecomunicación, *hardware* y *software* y servicios auxiliares que intervengan en el funcionamiento u operación de redes 5G o en la prestación de servicios 5G, detectando vulnerabilidades y amenazas que le afecten tanto a la gestión de la empresa como a dichos equipos, *hardware*, *software* y servicios.

2. Los suministradores 5G deberán aportar este análisis de riesgos al Ministerio para la Transformación Digital y de la Función Pública, cuando sea requeridos para ello. Asimismo, los suministradores 5G deberán aportar los análisis de riesgos a los operadores 5G a los que suministre de conformidad con lo dispuesto en el artículo 18.4.

3. No obstante lo dispuesto en el apartado anterior, los suministradores 5G que hayan sido calificados de alto riesgo o de riesgo medio deberán remitir al Ministerio para la Transformación Digital y de la Función Pública un análisis de riesgos de sus equipos, productos o servicios involucrados en las redes y servicios 5G en el plazo de seis meses a contar desde que hayan sido calificados de alto riesgo o de riesgo medio.

4. Los suministradores 5G que sean calificados de alto riesgo o de riesgo medio deberán llevar a cabo el análisis de riesgos cada dos años y remitirlo al Ministerio para la Transformación Digital y de la Función Pública o cuando le sea requerido para ello por el Ministerio para la Transformación Digital y de la Función Pública o siempre que se hayan producido cambios significativos en las infraestructuras 5G utilizadas o servicios 5G prestados que induzcan a pensar que las medidas de seguridad adoptadas pudieran haber perdido eficacia.

5. Los suministradores 5G son los responsables de los análisis de riesgos que efectúen y del cumplimiento de las obligaciones de información y remisión de documentación establecidos en este artículo.

Artículo 20. *Análisis de riesgos por los usuarios corporativos 5G.*

1. Los usuarios corporativos 5G que tengan otorgados derechos de uso del dominio público radioeléctrico para instalar, desplegar o explotar una red privada 5G o prestar servicios 5G para fines profesionales o en autoprestación deberán analizar los riesgos de las redes y servicios 5G, detectando vulnerabilidades y amenazas que afecten a los elementos de red, infraestructuras, recursos, facilidades y servicios que empleen o provean en la instalación, despliegue y explotación de redes privadas 5G o en la prestación de servicios 5G en autoprestación.

2. Los usuarios corporativos 5G mencionados en el apartado anterior deberán aportar este análisis de riesgos al Ministerio para la Transformación Digital y de la Función Pública, cuando sean requeridos para ello.

Artículo 21. *Confidencialidad de la información sobre análisis de riesgos.*

1. El Ministerio para la Transformación Digital y de la Función Pública podrá recabar de los sujetos obligados la información necesaria para el análisis de riesgos.

2. Los sujetos obligados deben proporcionar la información en el plazo de quince días hábiles a contar desde el día siguiente al de la notificación del requerimiento de información.

3. El incumplimiento de los requerimientos de información formulados conforme a lo indicado en el apartado anterior cuando haya pasado un mes desde la finalización del plazo dado para su cumplimiento es calificado como infracción grave.

4. Se garantizará la confidencialidad de la información que los sujetos obligados proporcionen sobre el análisis de riesgos y que no podrá ser utilizada para una finalidad distinta del cumplimiento de los objetivos y obligaciones establecidas en el Real Decreto-ley 7/2022, de 29 de marzo, en este esquema y en los actos que se dicten en ejecución de ambas disposiciones.

CAPÍTULO V

Gestión de los riesgos por los sujetos obligados

Artículo 22. *Medidas comunes para la gestión de seguridad.*

1. Las medidas a las que se hace referencia en este esquema se fundamentan en un enfoque basado en compendiar los riesgos cuya prevención, detección y mitigación o eliminación tenga por objeto proteger los sistemas, redes y servicios 5G, e incluirán al menos los siguientes elementos:

a) Las políticas de seguridad de los sistemas, redes y servicios 5G.
b) Análisis de riesgos.
c) La gestión de incidentes.
d) La continuidad de las actividades, como la gestión de copias de seguridad y la recuperación en caso de catástrofe, y la gestión de crisis.
e) La seguridad de la cadena de suministro y, en su caso, la estrategia de diversificación, cuando proceda.
f) La seguridad en la adquisición, el desarrollo y el mantenimiento de los sistemas y redes 5G.
g) Las políticas y procedimientos relativos a la utilización de la criptografía y, en su caso, de cifrado.
h) La seguridad de los recursos humanos, las políticas de control de acceso y la gestión de activos.
i) El uso de soluciones de autenticación, comunicaciones de voz, vídeo y texto seguras y sistemas seguros de comunicaciones de emergencia, cuando proceda.
j) El uso de componentes certificados.
k) La protección de servicios y datos en la nube.
l) La monitorización de sistemas, redes y servicios.
m) La seguridad física.
n) La protección de la información.
ñ) La realización de evaluaciones periódicas de vulnerabilidades y pruebas de penetración para identificar y resolver o mitigar estas vulnerabilidades antes de que puedan ser explotadas.

2. Los sujetos obligados deberán adoptar medidas técnicas y de organización adecuadas para gestionar los riesgos existentes en la instalación, despliegue y explotación de redes 5G y en la prestación de servicios 5G, con base en lo establecido en el Real decreto-ley 7/2022, de 29 de marzo, en este Esquema y en los actos que se dicten en ejecución de ambas disposiciones.

Artículo 23. *Gestión de seguridad por los operadores 5G.*

1. Los operadores 5G deberán garantizar la instalación, despliegue y explotación seguros de redes públicas 5G y la prestación segura de servicios 5G disponibles al público mediante la aplicación de técnicas y procedimientos de operación y supervisión que garanticen la seguridad de redes y servicios 5G, así como el cumplimiento de la normativa en esta materia.
2. Los operadores 5G tienen las siguientes obligaciones de seguridad dirigidas a mitigar riesgos:

a) Adoptar medidas técnicas y operativas para garantizar la integridad física y lógica de las redes 5G o cualesquiera de sus elementos, infraestructuras y recursos, así como la continuidad en la prestación de servicios 5G.
b) Adoptar planes y medidas de contingencia específicas para asegurar la continuidad de otros servicios esenciales para la sociedad que dependan de las redes y servicios 5G.
c) Seleccionar e identificar a las personas, ya sea personal propio o de empresas contratadas, que puedan acceder a los activos físicos y lógicos de la red, y realizar el mantenimiento de registros de acceso.
d) Mantener las credenciales de usuario para el acceso a la red en posesión del operador.

e) Utilizar únicamente productos, recursos, servicios o sistemas certificados para la operación de las redes 5G, o en alguna de sus partes o elementos.

En particular, exigirán de los suministradores la certificación del esquema GSMA Network Equipment Security Assurance Scheme (NESAS) y las SCAS (Security Assurance Specification), de estos productos, recursos, servicios o sistemas certificado.

f) También exigirán de los suministradores los certificados de conformidad de estos elementos con los Esquemas Europeos de Certificación que puedan desarrollarse bajo el Reglamento 2019/881, del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación, bajo la normativa de requisitos horizontales de ciberseguridad para productos con elementos digitales o bajo cualquier otra legislación relacionada de la UE o nacional.

g) Cumplir las normas o especificaciones técnicas aplicables a redes y sistemas de información, de conformidad con las normas nacionales, europeas e internacionales.

Especialmente, se deberán cumplir con las medidas de seguridad aplicables a sistemas de información de categoría Alta contempladas en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad o en el Perfil de Cumplimiento Específico que resultara de aplicación o, en su caso, las recogidas en la norma técnica 27002:2022: Seguridad de la Información, ciberseguridad y protección de la privacidad-controles de seguridad de la información, de no estar comprendidas en el ámbito de aplicación del Esquema Nacional de Seguridad o en el Perfil de Cumplimiento Específico que resultara de aplicación.

h) Cumplir con los esquemas europeos de certificación de productos, servicios o sistemas, sean o no específicos de la tecnología 5G, que se empleen en la operación o explotación de redes y servicios 5G.

i) Hacer uso de herramientas y metodologías de análisis y gestión de riesgos reconocidas nacional o internacionalmente.

j) Someterse, a su costa, a una auditoría de seguridad ordinaria, al menos cada dos años, que verifique el cumplimiento de los requerimientos del ENS 5G.

Con carácter extraordinario, deberá realizarse dicha auditoría siempre que se produzcan modificaciones sustanciales que puedan repercutir en las medidas de seguridad requeridas. La realización de la auditoria extraordinaria determinará la fecha de cómputo para el cálculo de los dos años, establecidos para la realización de la siguiente auditoría regular ordinaria, indicados en el párrafo anterior.

El informe de auditoría deberá dictaminar sobre el grado de cumplimiento de este real decreto identificando los hallazgos de cumplimiento e incumplimiento detectados. Deberá, igualmente, incluir los criterios metodológicos de auditoría utilizados, el alcance y el objetivo de la auditoría, y los datos, hechos y observaciones en que se basen las conclusiones formuladas.

El resultado de esta auditoría será presentado al Ministerio para la Transformación Digital y de la Función Pública con una periodicidad bienal.

k) Establecer procedimientos apropiados para abordar las vulnerabilidades cuando se detecten.

l) Exigir a sus suministradores el cumplimiento de estándares de seguridad, desde el diseño de los productos y servicios hasta su puesta en funcionamiento.

m) Controlar su propia cadena de suministro y la estrategia de diversificación que haya diseñado.

n) Colaborar con el Centro de Operaciones de Seguridad 5G de referencia a que se refiere el artículo 41 para enviar los datos requeridos para la detección del estado de la ciberseguridad de las redes y servicios 5G en tiempo real.

3. En particular, los operadores 5G que sean titulares o exploten elementos críticos de una red pública 5G tienen adicionalmente las siguientes obligaciones:

a) Deberán diseñar una estrategia de diversificación en la cadena de suministro de los equipos de telecomunicación, sistemas de transmisión, equipos de conmutación o encaminamiento y demás recursos que permitan el transporte de señales en una red pública 5G que dé cumplimiento a lo dispuesto en el artículo 17.

b) No podrán utilizar en los elementos críticos de red equipos de telecomunicación, sistemas de transmisión, equipos de conmutación o encaminamiento y demás recursos, que permitan el transporte de señales, hardware, software o servicios auxiliares de suministradores que hayan sido calificados de alto riesgo conforme a lo dispuesto en el artículo 15.

c) No podrán utilizar en la red de acceso radio de una red pública 5G equipos de telecomunicación, sistemas de transmisión, equipos de conmutación o encaminamiento y demás recursos, que permitan el transporte de señales, hardware, software o servicios auxiliares de suministradores que hayan sido calificados de alto riesgo, en aquellas estaciones radioeléctricas con las que se proporcione cobertura en las ubicaciones, áreas y centros que se hayan identificado conforme a lo establecido en el artículo 16.

d) Deberán ubicar los elementos críticos de una red pública 5G dentro del territorio nacional, sin perjuicio de lo establecido en el artículo 6.

Estas obligaciones se aplican de forma exclusiva a los elementos de la red de acceso radio 5G según la definición del 3GPP mencionada en el anexo I.

4. Los operadores 5G que sean titulares o exploten elementos críticos de una red pública 5G deberán remitir al Ministerio para la Transformación Digital y de la Función Pública una nueva estrategia de diversificación en la cadena de suministro antes del 1 de octubre de 2024.

Asimismo, la estrategia de diversificación en la cadena de suministro deberá ser remitida al Ministerio para la Transformación Digital y de la Función Pública cada vez que sea objeto de modificación.

Igualmente, los operadores 5G que sean titulares o exploten elementos críticos de una red pública 5G deberán remitir al Ministerio para la Transformación Digital y de la Función Pública antes del 1 de octubre de cada año información sobre el estado de ejecución de la estrategia de diversificación en la cadena de suministro o cuando le sea requerido para ello por el Ministerio para la Transformación Digital y de la Función Pública siempre que se hayan producido cambios significativos en las infraestructuras 5G utilizadas o servicios 5G prestados que induzcan a pensar que las medidas de seguridad adoptadas pudieran haber perdido eficacia.

5. Los operadores 5G deberán remitir al Ministerio para la Transformación Digital y de la Función Pública una nueva descripción de las medidas técnicas y organizativas diseñadas y aplicadas para gestionar y mitigar los riesgos antes del 1 de octubre de 2024 y, a continuación, cada dos años o cuando le sea requerido para ello por el Ministerio para la Transformación Digital y de la Función Pública siempre que se hayan producido cambios significativos en las infraestructuras 5G utilizadas o servicios 5G prestados que induzcan a pensar que las medidas de seguridad adoptadas pudieran haber perdido eficacia.

Artículo 24. *Gestión de seguridad por los suministradores 5G.*

1. Los suministradores 5G deberán garantizar la seguridad de los equipos de telecomunicación, *hardware, software* o servicios auxiliares que proporcionen y que sean objeto de uso por las redes y servicios 5G.

2. Los suministradores 5G tienen las siguientes obligaciones de seguridad dirigidas a mitigar riesgos:

a) Cumplir estándares de seguridad desde el diseño de los equipos, productos y servicios hasta su puesta en funcionamiento.

En particular, es de aplicación la norma técnica ISO/IEC 27001: Gestión de Seguridad de la Información.

b) Reforzar la integridad del *software,* actualización y gestión de parches. Las partes implicadas acordarán los mecanismos para las actualizaciones periódicas de *software* y para dar respuesta a las vulnerabilidades de seguridad considerando el ciclo de vida de los equipos y el nivel de exposición a vulnerabilidades y los criterios de evaluación ajustados del mismo.

Acreditar la certificación de los productos, recursos, servicios o sistemas para la operación de las redes 5G, o en alguna de sus partes o elementos. En particular, deberán cumplir con la certificación del esquema GSMA Network Equipment Security Assurance

Scheme (NESAS) y las SCAS (Security Assurance Specification), para los elementos de la red 5G que resulte de aplicación y para los restantes cualquier otro esquema de aseguramiento de la seguridad equiparable.

También deberán disponer, en su caso, de las certificaciones recogidas en los Esquemas Europeos de Certificación que puedan desarrollarse bajo el Reglamento 2019/881, del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad), bajo la normativa de requisitos horizontales de ciberseguridad para productos con elementos digitales o bajo cualquier otra legislación relacionada de la UE o nacional.

Estas certificaciones deberán ser aportadas a los operadores para que den cumplimiento a lo establecido en el artículo 23, así como al Ministerio para la Transformación Digital y de la Función Pública.

c) Cumplir las normas o especificaciones técnicas aplicables a redes y sistemas de información, de conformidad con las normas nacionales, europeas e internacionales.

Especialmente, se deberán cumplir las medidas de seguridad aplicables a sistemas de información de categoría Alta contempladas en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad o en el Perfil de Cumplimiento Específico que resultara de aplicación o, en su caso, las recogidas en la norma técnica 27002:2022: Seguridad de la Información, ciberseguridad y protección de la privacidad-controles de seguridad de la información, de no estar comprendidas en el ámbito de aplicación del Esquema Nacional de Seguridad o en el Perfil de Cumplimiento Específico que resultara de aplicación.

d) Garantizar la aplicación de medidas de seguridad técnicas y organizativas estándar a través de un sistema de certificación.

e) Efectuar una auditoría de seguridad de sus equipos, productos y servicios.

En particular, los suministradores 5G deben presentar al Ministerio para la Transformación Digital y de la Función Pública con una periodicidad bienal una auditoria sobre la aplicación del esquema de certificación GSMA Network Equipment Security Assurance Scheme (NESAS) y las SCAS (Security Assurance Specification), para los elementos de la red 5G que resulte de aplicación y para los restantes elementos cualquier otro esquema de aseguramiento de la seguridad equiparable, además de la norma técnica ISO/IEC 27001: Gestión de Seguridad de la Información, el Real Decreto 311/2022, de 3 de mayo, por el que se regula Esquema Nacional de Seguridad, o en el Perfil de Cumplimiento Específico que resultara de aplicación, en la categoría de seguridad Alta, en caso de fabricar, importar, distribuir o prestar cualesquiera otros servicios, en redes públicas 5G.

Además, deberán someterse, a su costa, a una auditoría de seguridad ordinaria, al menos cada dos años, que verifique el cumplimiento de los requerimientos del ENS 5G.

Con carácter extraordinario, deberá realizarse dicha auditoría siempre que se produzcan modificaciones sustanciales que puedan repercutir en las medidas de seguridad requeridas. La realización de la auditoria extraordinaria determinará la fecha de cómputo para el cálculo de los dos años, establecidos para la realización de la siguiente auditoría regular ordinaria, indicados en el párrafo anterior.

El informe de auditoría deberá dictaminar sobre el grado de cumplimiento de este real decreto identificando los hallazgos de cumplimiento e incumplimiento detectados. Deberá, igualmente, incluir los criterios metodológicos de auditoría utilizados, el alcance y el objetivo de la auditoría, y los datos, hechos y observaciones en que se basen las conclusiones formuladas.

El resultado de esta auditoría será presentado al Ministerio para la Transformación Digital y de la Función Pública con una periodicidad bienal.

f) Proporcionar información sobre posibles injerencias de terceros en el diseño, operación y funcionamiento de sus equipos, productos y servicios.

g) Proporcionar a los operadores 5G y usuarios corporativos 5G la información y acreditar el cumplimiento de estándares de seguridad de equipos, productos y servicios que suministren. Colaborar para realizar una correcta monitorización o detección de la ciberseguridad por parte de los Centros de Operaciones de Seguridad 5G que puedan crear los sujetos obligados.

3. Los suministradores 5G deberán aportar al Ministerio para la Transformación Digital y de la Función Pública una descripción de las medidas técnicas y organizativas diseñadas y aplicadas para detectar, gestionar y mitigar los riesgos, cuando sean requeridos para ello.

4. No obstante lo dispuesto en el apartado anterior, los suministradores 5G que hayan sido calificados de alto riesgo o de riesgo medio deberán remitir al Ministerio para la Transformación Digital y de la Función Pública un informe de las medidas técnicas y organizativas diseñadas y aplicadas para gestionar y mitigar los riesgos en el plazo de seis meses a contar desde que hayan sido calificados de alto riesgo o de riesgo medio.

5. Los suministradores 5G de alto riesgo y de riesgo medio deberán remitir al Ministerio para la Transformación Digital y de la Función Pública cada dos años una descripción de las medidas técnicas y organizativas diseñadas y aplicadas para detectar, gestionar y mitigar los riesgos, o cuando le sea requerido para ello por el Ministerio para la Transformación Digital y de la Función Pública siempre que se hayan producido cambios significativos en las infraestructuras 5G utilizadas o servicios 5G prestados que induzcan a pensar que las medidas de seguridad adoptadas pudieran haber perdido eficacia.

6. Los suministradores 5G son los responsables de la definición y ejecución de las medidas de mitigación de riesgos que lleven a cabo y del cumplimiento de las obligaciones de información y remisión de documentación establecidos en este artículo.

Artículo 25. *Gestión de seguridad por los usuarios corporativos 5G.*

1. Los usuarios corporativos 5G que tengan otorgados derechos de uso del dominio público radioeléctrico para instalar, desplegar o explotar una red privada 5G o prestar servicios 5G para fines profesionales o en autoprestación deberán garantizar la instalación, despliegue y explotación seguros de redes privadas 5G y prestación segura de servicios 5G en autoprestación mediante la aplicación de técnicas y procedimientos de operación y supervisión que garanticen la seguridad de las redes y servicios 5G.

2. Los usuarios corporativos 5G mencionados deberán aportar al Ministerio para la Transformación Digital y de la Función Pública una descripción de las medidas técnicas y organizativas diseñadas y aplicadas para gestionar y mitigar los riesgos, cuando sean requeridos para ello.

Artículo 26. *Gestión de seguridad por las Administraciones públicas.*

1. Las Administraciones públicas incluidas en el ámbito de aplicación de este esquema deberán adoptar medidas técnicas y de organización adecuadas para gestionar los riesgos existentes en la instalación, despliegue y explotación de redes 5G y en la prestación de servicios 5G.

2. En particular, las administraciones públicas que quieran llevar a cabo la instalación, despliegue y explotación de redes 5G, ya sean públicas o privadas, o la prestación de servicios 5G, disponibles al público o en autoprestación, no podrán, por razones de seguridad nacional, utilizar equipos, productos y servicios proporcionados por suministradores de alto riesgo o riesgo medio.

3. Cada órgano o entidad de la Administración pública incluida en el ámbito de aplicación de este esquema contará con una política de seguridad referida a los sistemas, redes y servicios 5G, formalmente aprobada por el órgano competente. Esta política de seguridad podrá determinar la inclusión de la totalidad o una parte de órganos administrativos o entidades pertenecientes al sector público institucional en el ámbito de aplicación de una sola política de seguridad.

Artículo 27. *Gestión de seguridad por los Centros de Operaciones de Seguridad 5G.*

1. Los sujetos obligados podrán constituir Centros de Operaciones de Seguridad 5G, que adoptarán medidas técnicas, operativas y de organización adecuadas y proporcionadas para garantizar la preparación, la capacidad de respuesta y la recuperación frente a incidentes, incluida la cooperación entre los sectores público y privado, así como para gestionar los riesgos que se planteen para la seguridad de los sistemas, redes y servicios 5G, para lo que deberán adoptar medidas para gestionar estos riesgos conforme a lo previsto en este esquema.

2. Las medidas a las que se hace referencia en el apartado anterior se fundamentarán en un enfoque holístico de los riesgos, la probabilidad de que produzcan los incidentes y su gravedad, incluidas sus repercusiones sociales y económicas, e incluirán, al menos, los siguientes elementos:

a) Las políticas de seguridad de cada elemento de la red y su correspondiente análisis de riesgos.
b) El procedimiento de gestión en caso de incidentes.
c) El análisis de la continuidad de las actividades, la gestión de copias de seguridad y la recuperación en caso de catástrofe, y la gestión de crisis.
d) La seguridad de la cadena de suministro, incluidos los aspectos de seguridad relativos a las relaciones entre cada sujeto obligado y sus proveedores o prestadores de servicios directos.
e) La seguridad en la adquisición, el desarrollo y el mantenimiento de los sistemas, redes y servicios 5G, incluida la gestión y divulgación de las vulnerabilidades.
f) Las políticas y los procedimientos para evaluar la eficacia de las medidas para la gestión de riesgos de ciberseguridad.
g) Las prácticas básicas de ciberhigiene y formación en ciberseguridad.
h) Las políticas y procedimientos relativos a la utilización de criptografía y, en su caso, de cifrado.
i) La seguridad de los recursos humanos, las políticas de control de acceso y la gestión de activos.
j) El uso de soluciones de autenticación multifactorial o de autenticación continua, comunicaciones de voz, vídeo y texto y sistemas seguros de comunicaciones de emergencia en la entidad, cuando proceda.
k) La monitorización o detección de la ciberseguridad en las redes y servicios 5G y entre sus componentes o su relación con otras redes.

3. Los sujetos obligados y los Centros de Operaciones de Seguridad 5G creados deberán colaborar y cooperar con el Centro de Operaciones de Seguridad 5G de referencia a que se refiere el artículo 41 en el desarrollo de sus funciones, a través de, entre otras, de las siguientes actuaciones:

a) Establecer mecanismos seguros de intercambio de información.
b) Llevar a cabo reuniones periódicas para tratar, entre otros asuntos, el estado de situación de la ciberseguridad 5G y estudiar posibles mejoras.
c) Designar una persona que ejercerá como punto de contacto con los responsables de la seguridad de la información nombrados por los sujetos obligados del sector de las telecomunicaciones en virtud del artículo 7 del RD 43/2021, por el que desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

Artículo 28. *Prestación de servicios de respuesta a incidentes de seguridad.*

1. La notificación de incidentes será llevada a cabo según los términos establecidos en el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información y en el Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, o en base a la normativa que pudiera remplazar a esta regulación fruto de la transposición de la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión.
2. El INCIBE-CERT, del Instituto Nacional de Ciberseguridad de España, prestará los servicios de respuesta a incidentes de seguridad que se produzcan en los sistemas, redes y servicios 5G de los sujetos obligados que no sean entidades del Sector Público y, en consecuencia, no estén incluidos en el ámbito subjetivo de aplicación de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
A tal efecto, en el ejercicio de este cometido, INCIBE-CERT ejercerá las funciones e implementará los procedimientos oportunos en los términos indicados en el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información y en el

Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

3. El CCN-CERT prestará los servicios de respuesta a incidentes de seguridad que se produzcan en los sistemas, redes y servicios 5G de los sujetos obligados que sean entidades del Sector Público y, en consecuencia, estén incluidos en el ámbito subjetivo de aplicación de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

A tal efecto, en el ejercicio de este cometido, CCN-CERT ejercerá las funciones e implementará los procedimientos oportunos en los términos indicados en el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información y en el Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

4. El ESPDEF-CERT, del Mando Conjunto del Ciberespacio, cooperará con el CCN-CERT y el INCIBE-CERT en aquellas situaciones que éstos requieran en apoyo de los operadores 5G y, necesariamente, en aquellos operadores que tengan incidencia en la Defensa Nacional.

5. La cooperación y coordinación oportunas entre INCIBE-CERT, CCN-CERT y ESPDEF-CERT se llevará a cabo conforme a lo indicado en el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información y en el Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

6. Mediante orden del Ministerio para la Transformación Digital y de la Función Pública se establecen la tipología de incidentes y los protocolos de actuación y comunicación para que el Ministerio para la Transformación Digital y de la Función Pública, a través del Centro de Operaciones de Seguridad 5G de referencia, conozca de los incidentes de seguridad que se produzcan en los sistemas, redes y servicios 5G de los sujetos obligados.

Artículo 29. *Condiciones de cumplimiento de las obligaciones.*

En el cumplimiento de las obligaciones establecidas en los artículos anteriores, los sujetos obligados tendrán en cuenta y aplicarán lo establecido en el Real Decreto-ley 7/2022, de 29 de marzo, en este esquema y en los actos que se dicten en ejecución de ambas disposiciones.

Artículo 30. *Confidencialidad de la información sobre gestión de riesgos.*

1. El Ministerio para la Transformación Digital y de la Función Pública podrá recabar de los sujetos obligados la información necesaria para la gestión de riesgos.

2. Los sujetos obligados deben proporcionar la información en el plazo de quince días hábiles a contar desde el día siguiente al de la notificación del requerimiento de información.

3. El incumplimiento de los requerimientos de información formulados conforme a lo indicado en el apartado anterior, cuando haya pasado un mes desde la finalización del plazo dado para su cumplimiento, es calificado como infracción grave.

4. Se garantizará la confidencialidad de la información que los sujetos obligados proporcionen sobre el análisis de riesgos y que no podrá ser utilizada para una finalidad distinta del cumplimiento de los objetivos y obligaciones establecidas en el Real Decreto-ley 7/2022, de 29 de marzo, en este esquema y en los actos que se dicten en ejecución de ambas disposiciones.

CAPÍTULO VI

Otras medidas de cumplimiento en materia de la seguridad de las redes y servicios 5G

Artículo 31. *Deber de colaboración en la modificación y ejecución del ENS5G.*

Todos los sujetos obligados, así como las Administraciones públicas, los fabricantes, importadores, distribuidores y quienes pongan en el mercado y comercialicen equipos terminales y dispositivos para conectarse a una red 5G y poder prestar servicios 5G,

deberán prestar la colaboración y remitir la información que le sea requerida para la modificación y ejecución del ENS5G.

Artículo 32. *Certificación de equipos, productos y servicios 5G.*

Mediante orden de la persona titular del Ministerio para la Transformación Digital y de la Función Pública se podrá supeditar la utilización de un equipo, sistema, programa o servicio en concreto por los sujetos obligados a la previa obtención de una certificación establecida en virtud del Reglamento (UE) 2019/881, del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad), o de los esquemas de certificación y normas técnicas de certificación de equipos y productos 5G que a nivel europeo o internacional puedan aprobarse, o cualquier otra legislación de la UE o nacional que así lo requiera en caso de que no existan.

Artículo 33. *Procedimientos de determinación de la conformidad con el Esquema Nacional de Seguridad 5G.*

1. Los sujetos obligados serán objeto de un proceso para determinar su conformidad con el ENS5G. A tal efecto, precisarán de una auditoría para la certificación de su conformidad, sin perjuicio de la auditoría de la seguridad prevista en los artículos 23 y 24 que podrá servir asimismo para los fines de la certificación.

Tanto la auditoría prevista en los artículos 23 y 24 como la auditoría de certificación se realizarán en los términos que se determinen en la correspondiente Instrucción Técnica de Seguridad, que concretará asimismo los requisitos exigibles a las entidades certificadoras.

2. Los sujetos obligados a los que se refiere el apartado anterior darán publicidad, en los correspondientes portales de internet o sedes electrónicas a las certificaciones de conformidad con el ENS5G, atendiendo a lo dispuesto en la mencionada Instrucción Técnica de Seguridad.

Artículo 34. *Cumplimiento de la normativa sobre inversiones extranjeras y sobre competencia.*

Las obligaciones establecidas en el Real Decreto-ley 7/2022, de 29 de marzo, en este esquema y en los actos que se dicten en ejecución de ambas disposiciones se entienden sin perjuicio de la aplicación de los instrumentos de control sobre inversiones extranjeras directas, así como de la aplicación de la normativa en materia de defensa de la competencia.

Artículo 35. *Equipos terminales.*

La fabricación, importación, distribución, puesta en el mercado y comercialización de equipos terminales y dispositivos para conectarse a una red 5G y poder prestar servicios 5G, estará condicionado al cumplimiento de los requisitos de seguridad para los productos digitales y de los requisitos esenciales aplicables relacionados con la ciberseguridad, adoptados conforme a la normativa europea, en particular, en relación con la protección de los datos personales, la privacidad, y la protección contra el fraude.

Artículo 36. *Cooperación internacional.*

1. El Gobierno y el Ministerio para la Transformación Digital y de la Función Pública cooperará estrechamente con las instituciones de otros Estados miembros de la Unión Europea y con las instituciones de la Unión Europea en la propuesta de modificación y ejecución del Esquema Nacional de Seguridad de redes y servicios 5G y, en general, colaborará con las distintas organizaciones internacionales especializadas para poder llevar a cabo un tratamiento integral y global de la seguridad de las redes y servicios 5G.

2. En particular, el Gobierno y el Ministerio para la Transformación Digital y de la Función Pública podrán compartir información relacionada con los análisis que realicen las instituciones de la Unión Europea y con otros Estados miembros de la Unión Europea preservando, como corresponda en Derecho, la seguridad, los intereses comerciales y la confidencialidad de la información recabada en la elaboración del análisis, así como servirse de la información que le envíen otros Estados o las instituciones de la Unión Europea para

su realización. Igualmente, podrá llevar a cabo estos análisis de forma conjunta con otros Estados miembros de la Unión Europea.

Artículo 37. *I+D+i en ciberseguridad 5G.*

El Ministerio para la Transformación Digital y de la Función Pública, directamente o a través del Centro de Operaciones de Seguridad 5G de referencia, impulsará la I+D+i en ciberseguridad 5G mediante la ejecución de distintos programas en los que se seguirán las siguientes líneas generales:

a) Establecimiento de programas de investigación y desarrollo I+D+i en ciberseguridad 5G, con el objetivo de promover la innovación y el desarrollo de tecnologías avanzadas para proteger las redes y servicios 5G contra posibles amenazas y ciberataques.

b) Convocatoria de ayudas públicas para financiar proyectos de investigación en ciberseguridad 5G, con el fin de impulsar la generación de conocimiento y la colaboración entre diferentes actores del sector.

c) Fomento de la colaboración público-privada en I+D+i en ciberseguridad 5G, a través de la creación de programas de financiación conjunta, la organización de eventos y la facilitación de la transferencia de tecnología entre empresas e instituciones de investigación.

d) Establecimiento de programas de apoyo específicos para startups y empresas emergentes que desarrollen soluciones innovadoras en ciberseguridad 5G, proporcionando financiación, y acceso a infraestructuras y recursos de investigación.

e) Promoción de la formación y capacitación de personal especializado en ciberseguridad 5G, en colaboración con los Ministerios competentes, para la creación de programas de formación universitaria y profesional, la organización de cursos y seminarios especializados, y el fomento de la participación en programas de becas y prácticas en empresas del sector.

f) Establecimiento de estándares y buenas prácticas en ciberseguridad 5G, con el objetivo de garantizar la interoperabilidad, la seguridad y la protección de la privacidad en las redes y servicios 5G.

Artículo 38. *Impulso a la interoperabilidad.*

El Ministerio para la Transformación Digital y de la Función Pública, directamente o a través del Centro de Operaciones de Seguridad 5G de referencia impulsará la interoperabilidad de los equipos y programas ligados a la gestión de redes y servicios 5G, así como la participación de actores públicos y privados en la elaboración de estándares sobre el funcionamiento de las redes y servicios 5G a través de las siguientes iniciativas:

a) Aprobación de normativas y directrices claras para promover la interoperabilidad de los equipos y programas relacionados con la gestión de redes y servicios 5G, incluyendo la definición de estándares técnicos y protocolos de comunicación que faciliten la integración y la compatibilidad entre diferentes sistemas y dispositivos.

b) Impulso para la adopción de estándares abiertos en el diseño y desarrollo de equipos y programas para redes y servicios 5G, con el objetivo de facilitar la interoperabilidad y evitar la dependencia de tecnologías propietarias.

c) Creación de espacios de colaboración entre actores públicos y privados para discutir y elaborar estándares sobre el funcionamiento de las redes y servicios 5G.

d) Promoción de la interoperabilidad como un criterio de evaluación en los procesos de contratación pública relacionados con la adquisición de equipos y servicios para redes y servicios 5G. Esto podría incentivar a los proveedores a desarrollar soluciones compatibles y facilitar la integración de sistemas heterogéneos en entornos públicos.

CAPÍTULO VII

Aplicación del ENS5G

Artículo 39. *Competencia para la aplicación del ENS5G.*

1. El Ministerio para la Transformación Digital y de la Función Pública será el departamento competente para aplicar el ENS5G y ejercer las demás funciones que le atribuye el Real Decreto-ley 7/2022, de 29 de marzo.

2. El Ministerio para la Transformación Digital y de la Función Pública, para el ejercicio de estas funciones, contará con el apoyo y asistencia del Centro de Operaciones de Seguridad 5G de referencia a que se refiere el artículo 41.

3. Asimismo, el Ministerio para la Transformación Digital y de la Función Pública, para la respuesta a incidentes de seguridad, contará con la cooperación de INCIBE-CERT, CCN-CERT y ESPDEF-CERT.

4. El Ministerio para la Transformación Digital y de la Función Pública se coordinará con los demás órganos competentes en materia de ciberseguridad e infraestructuras críticas para garantizar una aplicación coherente del ENS5G.

Artículo 40. *Facultades del Ministerio para la Transformación Digital y de la Función Pública para la aplicación del ENS5G.*

1. El Ministerio para la Transformación Digital y de la Función Pública, en el ejercicio de las funciones que le asigna el Real Decreto-ley 7/2022, de 29 de marzo, y el ENS5G podrá ejercer, entre otras, las siguientes facultades:

a) Desarrollar, concretar y detallar el contenido del ENS5G.

b) Autorizar la instalación, modificación o adaptación de estaciones radioeléctricas que proporcionen cobertura a determinadas ubicaciones, áreas y centros en los términos establecidos en el artículo 16.4.

c) Formular requerimientos de información a los sujetos obligados, que deberán ser respondidos en el plazo de 15 días hábiles a contar desde el día siguiente al de su notificación, a efecto de poder ejercer las funciones que le asigna el Real Decreto-ley 7/2022, de 29 de marzo, el ENS5G y su normativa de desarrollo y, en concreto, para verificar y controlar el cumplimiento de las respectivas obligaciones que se imponen a los sujetos obligados.

d) Realizar auditorías u ordenar su realización para verificar y controlar el cumplimiento de las respectivas obligaciones que el Real Decreto-ley 7/2022, de 29 de marzo, el ENS5G y su normativa de desarrollo impone a los sujetos obligados.

e) Realizar inspecciones por los funcionarios destinados en la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales y ejercer la potestad sancionadora en los términos indicados en el capítulo siguiente.

f) Conceder ayudas públicas.

g) Desarrollar iniciativas, para fomentar la investigación y el desarrollo en materia de seguridad en las redes y servicios 5G y para la formación de personal especializado.

h) Crear laboratorios que recreen entornos de redes y servicios 5G reales e independientes para el análisis y gestión de riesgos de seguridad y para el aseguramiento del cumplimiento de los requisitos del ENS5G.

i) Ejercer las demás funciones que le correspondan según la legislación aplicable.

2. El Ministerio para la Transformación Digital y de la Función Pública, para el ejercicio de estas funciones, contará con el apoyo y asistencia del Centro de Operaciones de Seguridad 5G de referencia a que se refiere el artículo 41.

Artículo 41. *Centro de Operaciones de Seguridad 5G de referencia.*

1. Dependiendo del Ministerio para la Transformación Digital y de la Función Pública se crea el Centro de Operaciones de Seguridad 5G de referencia, órgano de apoyo y supervisión de las actuaciones conducentes a garantizar la seguridad de los sistemas, redes y servicios 5G.

2. El Centro de Operaciones de Seguridad 5G de referencia tiene las siguientes funciones:

a) Contribuir y apoyar al ejercicio de las facultades que al Ministerio para la Transformación Digital y de la Función Pública se le asignan en el artículo 40.

b) Proporcionar apoyo operativo a los sujetos obligados en actividades vinculadas a la prevención, protección, detección y respuesta frente a amenazas, incidentes y ciberataques a los sistemas, redes y servicios 5G, así como en la certificación y normalización de los mismos.

c) Fomentar la prevención de los sistemas, redes y servicios 5G mediante actividades dirigidas a ampliar el conocimiento respecto de las vulnerabilidades, tanto técnicas como humanas, y reducir la superficie de exposición, como pueden ser la realización de auditorías, de inspecciones técnicas de seguridad, la gestión de vulnerabilidades, el análisis de vulnerabilidades automatizados o no. el registro y seguimiento de las vulnerabilidades identificadas, el seguimiento a la publicación de vulnerabilidades específicas relacionadas con el 5G, y apoyo a la puesta en práctica de remedios de dichas vulnerabilidades.

d) Capacitación y formación específica en materia de ciberseguridad 5G.

e) Asesorar a los sujetos obligados y sus Centros de Operaciones de Seguridad 5G sobre el diseño de las medidas de seguridad, de las herramientas a utilizar, el desarrollo de guías específicas y la aplicación de las medidas de protección.

f) Ofrecer servicios de seguimiento en el funcionamiento y operatividad de los sistemas, redes y servicios 5G para detectar y responder rápidamente a posibles amenazas y ciberataques.

g) Contribuir a la respuesta de incidentes de seguridad.

h) Desarrollar Planes y Procedimientos de Gestión de Crisis de ciberseguridad y Planes de Contingencia 5G a nivel nacional.

i) Proporcionar apoyo en la obtención de las certificaciones tanto de ámbito nacional como europeo.

j) Identificar y difundir mejores prácticas de implementación de ciberseguridad 5G entre los sujetos obligados.

k) Elaborar guías y documentos de mejores prácticas para la implementación y operación de los sistemas, redes y servicios 5G, abordando aspectos como la seguridad, la privacidad y la gestión de riesgos.

l) Evaluar el impacto de los estándares y normativa en materia de ciberseguridad 5G, proporcionando información y asesoramiento a los responsables de formular políticas para garantizar un entorno propicio para la adopción y el desarrollo de la tecnología 5G.

m) Llevar a cabo actividades de I+D+i en el ámbito de la ciberseguridad 5G, para detectar, anticipar, prevenir y mejorar la respuesta ante incidentes potenciales.

n) Cualquier otra función que se le asigne por el Ministerio para la Transformación Digital y de la Función Pública.

3. Para el ejercicio de estas funciones, el Centro de Operaciones de Seguridad 5G de referencia se integra en la estructura de ciberseguridad nacional en el marco del Sistema de Seguridad Nacional, podrá celebrar los oportunos convenios y mecanismos de colaboración con entidades especializadas en materia de ciberseguridad y protección de operadores 5G y, en su caso, protección de las entidades críticas, entre otros, el Instituto Nacional de Ciberseguridad de España, el Mando Conjunto del Ciberespacio, el Centro Criptológico Nacional, la Oficina de Coordinación de Ciberseguridad y el Centro Nacional de Protección de Infraestructuras Críticas del Ministerio del Interior.

CAPÍTULO VIII

Inspección y régimen sancionador

Artículo 42. *Facultades de inspección.*

El Ministerio para la Transformación Digital y de la Función Pública ejercerá en la aplicación y supervisión de lo establecido en el Real Decreto-ley 7/2022, de 29 de marzo, el ENS5G y su normativa de desarrollo todas las potestades de la función inspectora previstas

en dichas normas y en el título VIII de la Ley 11/2022, de 28 de junio, General de Telecomunicaciones.

Artículo 43. *Régimen sancionador.*

Será de aplicación el régimen sancionador establecido en los artículos 30 y 31 del Real Decreto-ley 7/2022, de 29 de marzo.

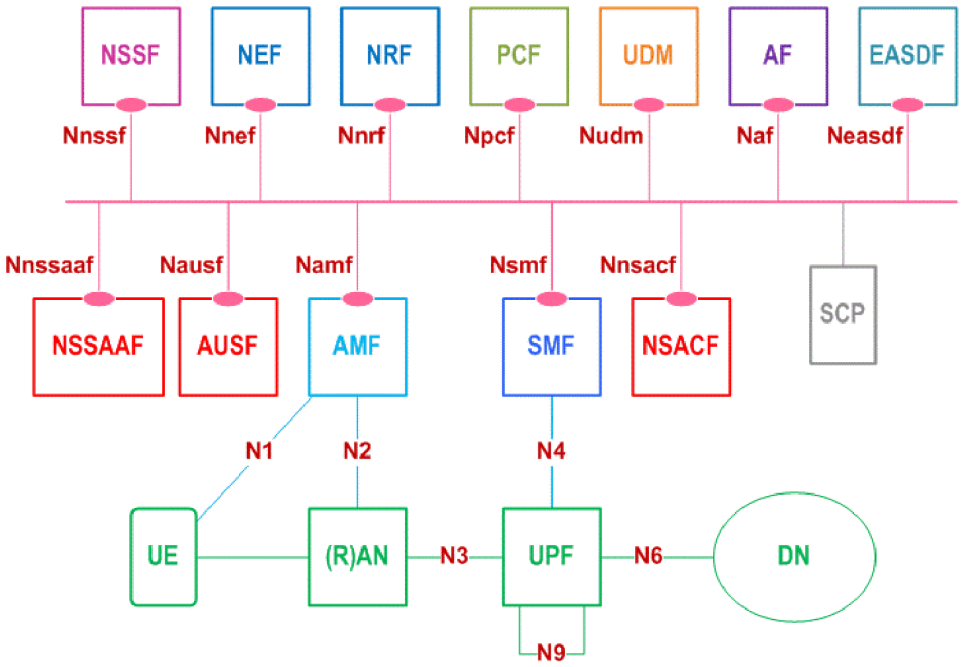
ANEXO I

Elementos, infraestructuras y recursos que integran una red 5G

1. Descripción de la arquitectura de la red 5G-SA

Para el análisis requerido en el presente Esquema Nacional de Seguridad de redes y servicios 5G, se utiliza una arquitectura de red de referencia, siguiendo la recomendación del 3GPP y la especificación ETSI TS 123 501.

En la figura siguiente, se muestra un esquema simplificado de una arquitectura 5G-SA para escenarios de no-roaming (que será utilizada de forma genérica como base). Elementos no presentados en la figura son el UDR, UDSF, UCMF, CHF, 5G-EIR, NWDAF y SEPP.



Estos elementos de red son funciones software que se despliegan sobre una infraestructura de virtualización (compuesta, a su vez, de hardware y software de virtualización), la cual puede ser dedicada y específica para una función de red, o común para varias funciones, incluso funciones de red de varios suministradores 5G. En este escenario, la infraestructura para hospedar las funciones de red virtualizadas puede estar diversificada tanto geográficamente como por suministradores 5G diferentes, tal y como se describirá más adelante en este documento.

Adicionalmente a los elementos de red, se despliegan un conjunto de Sistemas para la operación y gestión de la red GER (también denominados OSS, Operations Support System).

2. Identificación y descripción de los entornos de red 5G-SA

Con el objetivo de desglosar la complejidad de la arquitectura de una red 5G-SA, se divide la misma en entornos de red.

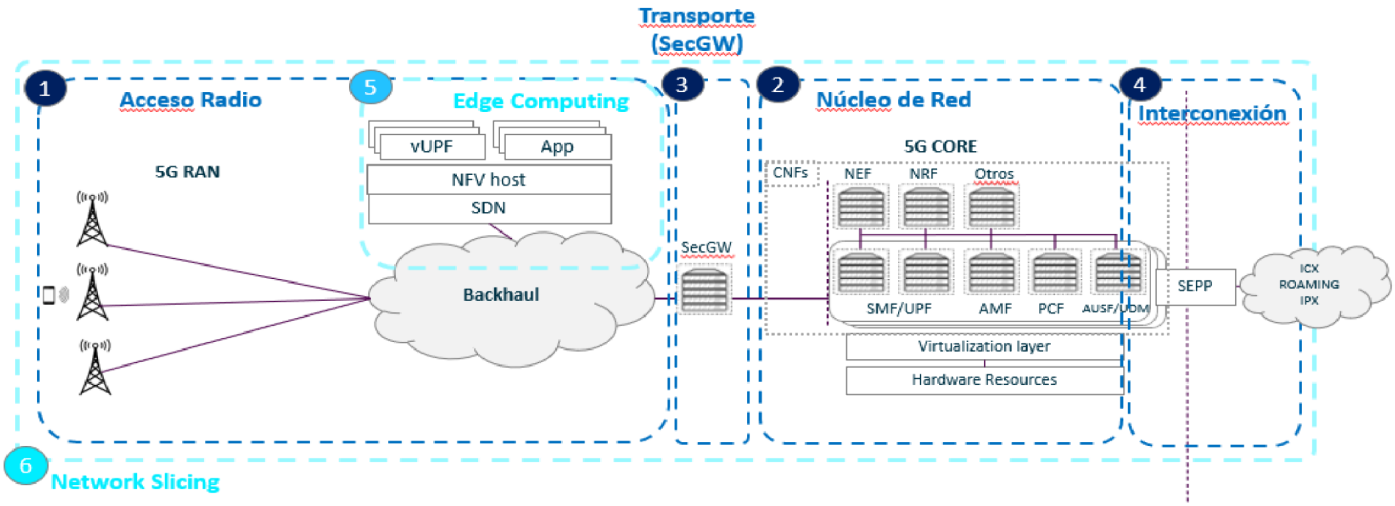
Un entorno de red es una agrupación de activos que tienen un cometido y unas características particulares dentro de la red que los diferencian del resto de entornos.

Se puede distinguir dos tipologías de entorno:

a) Entornos primarios: Se consideran entornos primarios aquellos propios de la tecnología o naturaleza de 5G que no existirían sin su despliegue.

b) Entornos secundarios: Se consideran entornos secundarios aquellos comunes en un operador de telecomunicaciones.

En la siguiente figura (figura 2) se puede apreciar una clasificación de la red 5G-SA por entornos:



3. Entornos de red primarios

Dentro de los entornos de red primarios, se encuentra el Acceso Radio, el Núcleo de Red, el Transporte-Backhaul (SecGW), la Interconexión de Roaming y los Sistemas de Control, Gestión y Operación de la Red.

a) Acceso Radio: El entorno de acceso radio (RAN) se encarga de dotar de cobertura a los terminales para que estos se puedan conectar a la red. Destacan las siguientes funciones en el entorno:

1. Operación y mantenimiento del emplazamiento radio. El software permite configurar cada emplazamiento con una serie de células por tecnología para poder prestar servicio a los usuarios y, durante el funcionamiento de la estación base, supervisa su estado para detectar posibles problemas o averías, ante cuya aparición reportaría una alarma al sistema de gestión para que el operador sea consciente y resuelva el problema.

2. Señalización. Para que los usuarios puedan registrarse en la red y establecer servicios portadores para sus comunicaciones, es necesaria señalización entre los terminales, la estación base, y el núcleo de red, y parte de estas funciones las realiza el software de la estación base.

3. Gestión de recursos radio. Los recursos radio de una célula dada son compartidos entre distintos usuarios y el software de la estación base es el responsable de repartirlos entre dichos usuarios (calidad del enlace radio de cada usuario, demanda de velocidad, etc.). El software también puede distribuir a los usuarios entre las células de su estación base (o incluso con células de emplazamientos vecinos), para que el reparto de usuarios sea más homogéneo entre células vecinas.

4. Movilidad. el software de la estación base gestiona el traspaso de las comunicaciones de los usuarios entre distintas células, de su emplazamiento o de emplazamientos vecinos, a medida que los usuarios se desplazan por la red.

5. Transporte: La comunicación física con el resto de la red se realiza por medio de enlaces IP, eléctricos u ópticos, y la estación base tienen que encargarse de gestionar dichos enlaces (priorización entre los distintos tipos de tráfico que van por dichos enlaces, configuración de VLANs, supervisión del enlace, etc.).

La red 5G, en el plano de acceso radio (RAN), se implementa con un solo tipo de elemento de red denominado, de forma genérica, gNodoB (gNB). La mayoría de los suministradores 5G de Red de acceso radio disponen de distintos modelos de gNB, adaptados a distintos tipos de escenarios.

De forma genérica, existen los tipos siguientes:

1. Macro gNB: proporcionan mayor área de cobertura y capacidad de tráfico. Se instalan típicamente en azoteas de edificios o lugares con mucha visibilidad radioeléctrica, con el objetivo de dar cobertura y capacidad general.

2. Micro gNB: de menor potencia, orientados a dar cobertura en localizaciones concretas, ya sean pequeños espacios públicos (como plazas) o espacios de interior (como lugares de eventos, oficinas pequeñas, etc.), o bien para dar capacidad complementaria a la capa general o macro. Se instalan principalmente en puntos de alta demanda de capacidad, para absorber dicha demanda.

3. Sistemas gNB de cobertura de interiores: especializados en cubrir espacios de interiores grandes, con numerosos puntos radiantes de baja potencia, para distribuir la cobertura 5G por dicho espacio interior. Se instalan típicamente en grandes edificios de oficinas, estadios deportivos, metros, etc.

En este contexto, un emplazamiento de la Red de acceso radio 5G estará compuesto por una banda base y varias cabezas remotas y/o antenas activas. El número de cabezas remotas y antenas activas dependerá del número de bandas presentes en el emplazamiento, y del número de sectores.

El software del gNB es común a la banda base, a las cabezas remotas y a las antenas activas, y también es común entre los distintos sistemas de comunicaciones móviles presentes en el emplazamiento (2G, 3G, 4G y/o 5G). Mediante la interfaz NG la estación base se comunica con el Núcleo de red y mediante la interfaz aire con los terminales móviles.

b) Núcleo de red: El núcleo de la red 5G-SA se compone de una serie de funciones de red estandarizadas por el 3GPP que se comunican entre ellas por conexiones tipo SBI (Service Based Interfaces), permitiendo un mallado total en función de las necesidades de cada una de ellas.

Los principios clave de esta arquitectura 5G-SA son:

1. Separar las funciones del plano de usuario (UP) de las funciones del plano de control (CP), lo que permite escalabilidad independiente, evolución e implementaciones flexibles, por ejemplo, ubicación centralizada o ubicación distribuida (remota).

2. Modularizar el diseño de la función, por ejemplo, para permitir un corte de red flexible y eficiente.

3. Permitir que cada Función de Red (y sus Servicios asociados) interactúen con otras Funciones de red, directa o indirectamente a través de un *Proxy*.

4. Integrar diferentes tipos de acceso, por ejemplo, acceso 3GPP y acceso no 3GPP.

5. Soporta un marco de autenticación unificado.

6. Desacoplar en las funciones de red las funciones de lógica de tipo «stateless» y relacionadas con capacidad de cómputo, de las funciones de estado de tipo «statefull» relacionadas con capacidades de almacenamiento.

7. Permitir la exposición de datos de red de forma segura para el desarrollo de nuevos servicios en base a ellos.

8. Soporte de acceso simultáneo a servicios locales (con requisitos de baja latencia) y servicios centralizados.

9. Permitir y aceptar la itinerancia de tráfico con otras redes, según diferentes modelos de arquitectura.

El conjunto de funciones de núcleo de red definidas por el 3GPP es el siguiente:

1. AMF-Access and Mobility Management Function: función del plano de control de la red 5G. Sus principales funciones son la gestión del registro, la gestión de la movilidad, la gestión de la conexión, y la gestión de diversos aspectos relacionados con la seguridad y autorización de los accesos.

2. SMF-Session Management Function: función del plano de control que se encarga de la gestión de las sesiones (establecimiento, modificación y liberación), gestión y asignación de IP a los terminales de usuario. En resumen, es la responsable de interactuar con el plano de usuario, creando, actualizando o borrando sesiones PDU, a la vez que administra el contexto de la sesión con el UPF.

3. UPF-User Plane Function: función del plano de usuario. Es la responsable del reenvío, enrutamiento e inspección de paquetes, así como de la gestión de la calidad de servicio. Representa el punto de interconexión a la red de datos.

4. PFC-Policy Control Function: es la encargada de proporcionar reglas de políticas a las funciones de red del plano de control, incluyendo *network slicing, roaming,* gestión de movilidad, o políticas de calidad de servicio 5G. Para la ejecución de las políticas, accede a la información de suscripción del UDR.

5. NRF-Network Repository Function: es la encargada del descubrimiento de los servicios, y mantiene el perfil e instancias de red disponibles. Sus funciones principales son la gestión del servicio, el descubrimiento de servicios, y *access token,* permitiendo poner en comunicación a dos elementos de la red 5G.

6. SEPP-Security Edge Protection Proxy: es la función de red que permite una interconexión segura entre redes 5G, garantizando la confidencialidad y/o integridad de extremo a extremo entre la red de origen y la de destino, para todos los mensajes de *roaming* de interconexión 5G.

7. UDM-Unified Data Management: función del plano de control cuyas principales misiones son la generación de credenciales de autenticación, la gestión de identidades de usuario, la gestión de suscripción, la autorización de acceso basado en datos de suscripción, y almacenamiento y gestión de las funciones de red que dan servicio al usuario. El UDM utiliza los datos de suscripción almacenados en el UDR.

8. UDR-Unified Data Repository: es el repositorio unificado de datos de usuario. Estos datos se estructuran en diferentes categorías o tipos, y son accesibles a las diversas funciones de red mediante una serie de servicios expuestos para la gestión y consulta de los mismos (UDM, PCR, NRF…, entre otros).

9. AUSF-Authentication Server Function: es la función del plano de control de la red 5G que se encarga de la autenticación del usuario.

10. CHF-Charging Function: la funcionalidad de tarificación reside en el tarificador convergente (CCS, Converged Charging System), que ofrece las funcionalidades de tarificación online y offline. Entre sus funciones, está el OCF (Online Charging Function), para realizar el control online de las sesiones de datos, el CDF (Charging Data Function), para construir un CDR con la información de red recibida, el ABMF (Account Balance Management Function), para la gestión del saldo y controles de consumo, el RF (Rating Function), función para establecer un precio al uso recibido (tanto online como offline), y el CGF (Charging Gateway Function), para generar CDRs tarificados.

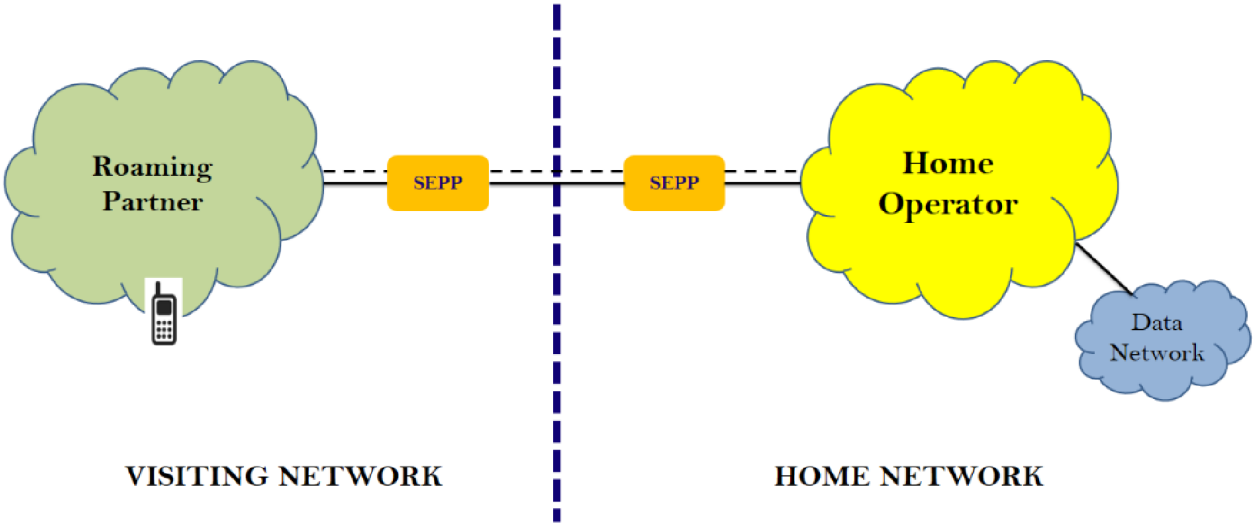
11. NEF-Network Exposure Function: proporciona un medio para exponer, de forma segura, los servicios y capacidades ofrecidos por las funciones de red de 5G.

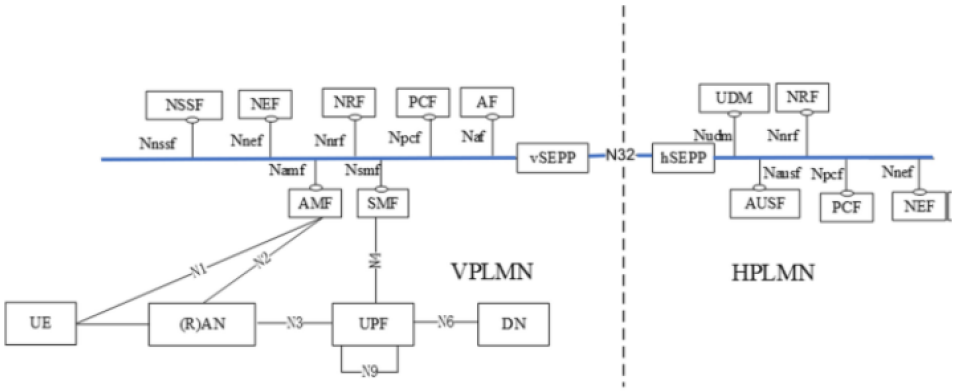
12. 5G-EIR-5G-Equipment Identity Register: es una funcionalidad opcional que ofrece la capacidad de chequear el estatus de la identidad del terminal (IMEI) y comprobar que no se encuentre en una lista negra.

c) Transporte-Backhaul (SecGW): El Security Gateway (SecGW) proporciona el cifrado del tráfico del plano de control y del plano de usuario entre los entornos de Acceso Radio y de Núcleo de Red, evitando además exposiciones innecesarias de elementos críticos.

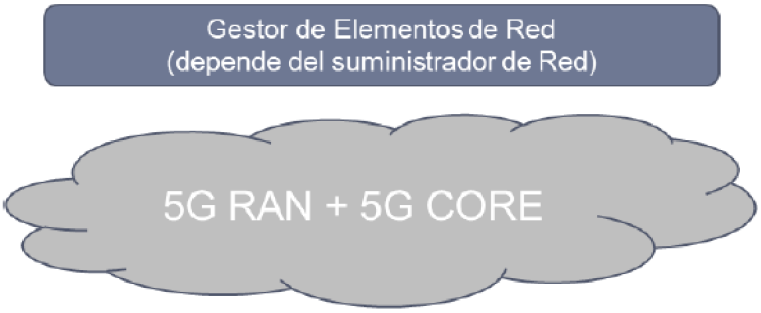
d) Interconexión Roaming: El entorno de Interconexión Roaming es necesario para la comunicación con el resto de los operadores de cara a permitir que un usuario de 5G pueda moverse de manera internacional ininterrumpiendo su servicio de voz o banda ancha.

En la siguiente figura (figura 3) se contiene la representación de un Entorno de Interconexión de Roaming:





e) Sistemas de Control, Gestión y Operación y Servicios de Apoyo: El proceso de aseguramiento del núcleo de red 5G se apoya en un conjunto de sistemas de apoyo a la operación (OSS) que se muestran en la siguiente figura (figura 4).



Estos sistemas OSS no forman parte de la prestación del servicio y, por tanto, fallos en su funcionamiento no afectan de forma directa a la disponibilidad de la red ni a la calidad del servicio prestado sobre ella. Sin embargo, la indisponibilidad de estos sistemas afectaría a la capacidad de supervisión, análisis, configuración y planificación de la red descrita en el punto anterior. Desde el punto de vista de la seguridad estos sistemas gestores están segmentados según el suministrador y por tanto una incidencia de seguridad en uno de ellos no afectaría a las funciones de red que no esté bajo el amparo de este OSS.

4. Entornos de red secundarios

Dentro de los entornos de red secundarios, se encuentran las Plataformas de Virtualización, la Infraestructura física, el *Edge-Computing* y el *Network Slicing.*

a) Plataformas de Virtualización y Orquestación: Muchos de los elementos de una red 5G son funciones «software» que se despliegan sobre una infraestructura de virtualización (que, a su vez, se compone de hardware y software de virtualización), la cual puede ser dedicada y específica para una función de red, o común para varias funciones (incluso funciones de red de varios suministradores). En este contexto, la infraestructura para hospedar las funciones de red virtualizadas está diversificada tanto geográficamente como por suministradores diferentes.

b) Infraestructura física: Los elementos y funciones de red pertenecientes a los distintos entornos requieren de una infraestructura física donde emplazarlos, cuya naturaleza, disponibilidad y seguridad dependerá obviamente de la criticidad del activo en concreto. Esta infraestructura física otorga a los elementos y funciones de red las necesidades básicas para un correcto funcionamiento.

c) MultiAccess Edge-Computing (MEC): El *edge computing* multiacceso es un tipo de arquitectura o entorno de red que pretende llevar las funciones de procesamiento de tráfico de usuario y *cloud computing* TI al extremo de la red con el objetivo garantizar el funcionamiento de nuevos casos de uso que requieren una latencia mínima.

En concepto, se define en términos más amplios como una evolución del *cloud computing* que utiliza las tecnologías móviles y de nube para separar los *hosts* de aplicaciones del centro de datos donde se encuentran y trasladarlos hacia el extremo de la red. Esto no sólo permite que los usuarios finales estén más cerca de las aplicaciones, sino también que los servicios informáticos estén más cerca de los datos que estas generan.

En este *Edge-Computing* conviven tanto aplicaciones de terceros, como funciones de red para procesar en el *Edge* el tráfico de usuario.

d) Network Slicing: Se trata de una forma de arquitectura que ofrece la posibilidad de crear, sobre una infraestructura física de virtualización común compartida, varias redes virtuales personalizadas y aisladas de manera lógica entre sí, otorgando a cada una de ellas una criticidad determinada en función de las necesidades específicas de aplicaciones, servicios, dispositivos, clientes u operadores.

Se prevé que, con esta tecnología, los operadores de redes y servicios 5G puedan implementar una segmentación de red para crear múltiples redes virtuales con diferentes tamaños de conectividad, adaptándose a las necesidades de conexión de los diferentes

usuarios, asignado de forma específica los recursos necesarios para garantizar el servicio correcto.

En líneas generales, dentro del concepto *network slicing,* cada red virtual (o porción de la red) engloba un conjunto independiente de funciones lógicas de red que soportan los requerimientos del caso de uso particular. Cada uno de ellos se optimizará para brindar los recursos y razonamientos matemáticos de red para el servicio y el tráfico que será usado en la segmentación.

En el caso de la tecnología 5G-SA, capacidad, conectividad, variedad, velocidad, cobertura y seguridad se asignarán para satisfacer las demandas específicas de cada caso de uso.

ANEXO II

Análisis de riesgos a nivel nacional

1. Metodología empleada

Un análisis de riesgos tiene como objetivo identificar y categorizar las principales amenazas sobre las redes y servicios 5G, con la finalidad de determinar medidas correctivas que puedan disminuir sus consecuencias o incluso evitarlas.

Conociendo esta finalidad, el paso siguiente lógico es establecer los medios para lograr dicho objetivo. Un análisis de riesgos ha de realizarse con una metodología estandarizada, holística y un orden consecuente y lógico, pormenorizando cada uno de los aspectos de manera cualitativa y cuantitativa. En caso contrario, el nivel de riesgo calculado podría desvirtuarse y con él, los criterios y prioridades en las medidas de protección y/o acciones clave a llevar a cabo.

Se muestra a continuación las fases seguidas para el análisis efectuado, así como las fuentes de información utilizadas para la metodología utilizada.

a) Identificación y descripción de la arquitectura 5G, los entornos de red existentes en la misma y los activos que la componen, todo ello sujeto a la evolución tecnológica (ver anexo I).

b) Identificación de criticidad para los activos dentro de cada una de las partes o elementos de una red 5G, sean partes o elementos críticos o no de la red 5G en los términos indicados en el artículo 6, apartados 2 y 3, del Real Decreto-ley 7/2022, de 29 de marzo, artículos 5 y 6 y anexo I de este esquema: para poder identificar el impacto de una amenaza en la red, es necesario primeramente determinar la criticidad de cada uno de los activos, basándonos en las cinco dimensiones de seguridad (Confidencialidad, Integridad, Trazabilidad, Autenticidad y Disponibilidad).

c) Identificación de los riesgos de la tecnología 5G y su impacto en los activos identificados: determinar las potenciales amenazas presentes en este entorno específico, clasificándolas por activo e identificando su nivel de riesgo.

d) Identificación de las medidas de seguridad técnicas, organizativas y estratégicas, para paliar o reducir el nivel de riesgo de las amenazas identificadas para cada entorno de red. Su efectividad será directamente proporcional al grado de disminución del nivel de riesgo para una determinada amenaza y activo.

e) Gestión de los riesgos y riesgos remanentes, en aquellas amenazas cuyo nivel sea considerable y no pueda ser disminuido por ninguna medida adicional desde el diseño (ver anexo III).

2. Dimensiones de seguridad que afectan a la criticidad de un activo

De manera estandarizada y ampliamente reconocida, se consideran cinco dimensiones de seguridad a la hora de evaluar la criticidad de los activos dentro de cada una de las partes o elementos de una red 5G, sean partes o elementos críticos o no de la red 5G en los términos indicados en el artículo 6, apartados 2 y 3, del Real Decreto-ley 7/2022, de 29 de marzo, artículos 5 y 6 y anexo I de este esquema, cuando de evaluar la seguridad de una solución es lo que aplica.

Las cinco dimensiones de seguridad son Confidencialidad, Integridad, Trazabilidad, Autenticidad y Disponibilidad.

a) Confidencialidad: La confidencialidad en un activo o una red valora la capacidad de evitar que la información que está contenida en el activo, o en tránsito en la red, sea expuesta a usuarios no autorizados, los cuales no deben tener acceso a ésta y la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

Las medidas de seguridad para garantizar la confidencialidad son diversas, desde la segmentación y el control de acceso, hasta el cifrado robusto de la información. El principal factor a la hora de valorar importancia de la confidencialidad en un activo es la sensibilidad de la información que almacena o transita por el mismo. Es importante tener en cuenta cuando se atiende a este factor, el impacto que puede tener para el resto de la red el hecho de que se comprometa ese activo.

Ejemplos de riesgos que puedan comprometer la confidencialidad son los siguientes: Espiar/interceptar el tráfico/datos de usuario en la red (Man in the Middle/, Eavesdropping), u obtener las credenciales de los operadores, ya sea debido a una errónea configuración de la red, a la ausencia de políticas de segmentación y control de acceso a los activos, o, por ejemplo, a la ausencia de cifrado en interfaces expuestas.

b) Integridad: La integridad es la capacidad de garantizar que los datos de un activo/usuario/red durante su ciclo de vida, ya sea en tránsito o almacenados, son modificados sólo por los agentes autorizados a ello, evitando que fuentes no deseadas puedan cambiar o manipular dichos datos, es decir, que no ha sido alterado de manera no autorizada. Algunas medidas para garantizar la integridad pueden ser la segmentación y el control de acceso, la comprobación del *hash* en los paquetes, la verificación de integridad de las versiones a instalar o almacenadas, etc.

Ejemplos de riesgos que comprometan la integridad son: Manipulación del tráfico/datos (en tránsito o almacenado) en interfaces expuestas de la red 5G.

c) Trazabilidad: propiedad o característica consistente en que las actuaciones de una entidad (activo/usuario/red/persona/proceso) pueden ser trazadas de forma indiscutible hasta dicha entidad.

Ejemplos de riesgos que puedan comprometer la trazabilidad son los siguientes: pérdida de control de la cadena de generación de información y/o datos o la manipulación y/o borrado de los registros y *logs*.

d) Autenticidad: propiedad o característica consistente en que una entidad (activo/usuario/red/persona/proceso) es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

Ejemplos de riesgos que puedan comprometer la autenticidad son los siguientes: falsificación de información y/o de paquetes de datos.

e) Disponibilidad: La disponibilidad se basa en el principio de garantizar que los usuarios legítimos tengan acceso ininterrumpido a los servicios y datos dentro del entorno para su correcto funcionamiento y las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. Este concepto pretende juzgar la importancia del activo y su solución en la continuidad de negocio de un determinado servicio, recurso o infraestructura. El nivel de riesgo de afectación a la disponibilidad se suele unir al número y al tipo de usuarios afectados que supondría la caída del servicio.

Para garantizar la disponibilidad se pueden tomar diversas medidas entre las que están la creación de soluciones de *backup,* la redundancia/resiliencia de los activos, la capacidad de mitigación frente a ataques DDoS, o los procedimientos eficaces de restauración del servicio tras la caída.

Dentro del entorno, algunos riesgos que puedan comprometer la disponibilidad son los siguientes: Ataques como denegación de servicio a la función de red, a la infraestructura de virtualización, o la infraestructura física, o catástrofes naturales, terrorismo, etc.

3. Determinación de la criticidad de los activos

Se procede, en este apartado, a identificar la criticidad de los activos de una red 5G-SA, teniendo en cuenta las cinco dimensiones de seguridad descritas en el apartado anterior.

1. Se definen tres categorías de criticidad de los activos: BÁSICA, MEDIA y ALTA.

a) Un activo será de categoría ALTA si alguna de sus dimensiones de seguridad alcanza el nivel de seguridad ALTO.

b) Un activo será de categoría MEDIA si alguna de sus dimensiones de seguridad alcanza el nivel de seguridad MEDIO, y ninguna alcanza un nivel de seguridad superior.

c) Un activo será de categoría BÁSICA si alguna de sus dimensiones de seguridad alcanza el nivel BAJO, y ninguna alcanza un nivel superior.

a) Red de acceso.

– gNB: Criticidad media.

Descripción del activo			Dimensión de Seguridad					Criticidad
Tipo	Dominio	Activo	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	
Primario	Red De Acceso	gNB	2 – Media	2 – Media	1 – Baja	2 – Media	2 – Media	2 – Media

Los nodos de acceso radio se encuentran ubicados, en su gran mayoría, en emplazamientos en lugares públicos no seguros. Esto hace que su exposición a ataques *in situ* aumente. La afectación de una celda puede suponer la interrupción de servicio en un área reducida, afectando a una cantidad de usuarios pequeña, además de poder ser soportado su tráfico por alguna otra estación base cercana, por lo que se considera que la criticidad es baja en cuanto a disponibilidad.

Estos nodos no almacenan datos de usuario. A pesar de ello, si se produce un ataque *Man in the Middle* (*MitM*), podría verse comprometido el tráfico no cifrado (afectando sólo a los pocos usuarios conectados a ese nodo), además de poder manipular los paquetes en curso si no existe verificación de integridad. Debido a la dificultad de realizar este ataque en el escenario descrito, a la confidencialidad, integridad y autenticidad se le otorga una criticidad media.

b) Núcleo de red.

– AUSF, UDM y UDR: Criticidad alta.

Descripción del activo			Dimensión de Seguridad					Criticidad
Tipo	Dominio	Activo	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	
Primario	Núcleo de red	UDM	3 – Alta	3 – Alta	3 – Alta	3 – Alta	3 – Alta	3 – Alta
		UDR	3 – Alta	3 – Alta	3 – Alta	3 – Alta	3 – Alta	3 – Alta
		AUSF	3 – Alta	3 – Alta	3 – Alta	3 – Alta	3 – Alta	3 – Alta

Un atentado contra la confidencialidad/integridad en estos activos puede suponer la exposición de información crítica del usuario en la red (claves de autenticación, integridad y cifrado, datos de provisión de los usuarios y sus identidades, etc.).

La obtención de esta información tendría un impacto muy alto debido a que es información asociada directamente a la tarjeta SIM de los clientes, y su exfiltración puede conllevar no sólo a una exposición de las comunicaciones de los usuarios, sino también a la pérdida de imagen del operador de redes y servicios 5G, y puede implicar la sustitución de las tarjetas SIM comprometidas. Por dichos motivos, la criticidad del activo en lo que a confidencialidad e integridad se refiere es alta.

Además, al ser un elemento centralizado que recibe las peticiones de autenticación de todos los usuarios de la red, en caso de no desplegarse con una solución correcta que garantice su resiliencia y continuidad de negocio, una disrupción en el mismo puede

provocar la caída completa de la red. Por tanto, en cuanto a disponibilidad, también tiene una criticidad alta.

En el caso de la autenticidad y trazabilidad se le otorga una criticidad alta.

– AMF, NRF y NEF: Criticidad alta.

Descripción del activo			Dimensión de Seguridad					Criticidad
Tipo	Dominio	Activo	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	
Primario	Núcleo de red	AMF	3 – Alta	2 – Media	2 – Media	2 – Media	2 – Media	3 – Alta
		NRF	3 – Alta	3 – Alta	1 – Baja	3 – Alta	3 – Alta	3 – Alta
		NEF	2 – Media	2 – Media	1 – Baja	2 – Media	2 – Media	2 – Media

• NRF: Criticidad alta.

Este elemento dispone de un mapa de toda la red, nodos y servicios. Un acceso no autorizado puede dar el detalle del despliegue de la red, los enrutamientos, DNS, *slices*, servicios, etc. Además, la alteración de su configuración puede provocar errores de comunicaciones internas en la red. Dadas estas razones, la confidencialidad e integridad del NRF se consideran de criticidad alta.

Sin embargo, dado que en casos de caída de NRF, el AMF guarda en caché los destinos de forma indefinida, hace que su criticidad en cuanto a disponibilidad sea baja.

En el caso de la autenticidad y trazabilidad se le otorga una criticidad alta.

• AMF: Criticidad alta.

Al ser el encargado de gestionar la movilidad de los usuarios, un ataque o acceso no autorizado puede permitir obtener o exfiltrar información delicada (identidades del usuario, localización a nivel de *Tracking Area*, e incluso el identificador del nodo donde se encuentra el cliente cuando el terminal está en modo conectado).

Por este motivo, riesgos de exfiltración más que de alteración de información, se considera alta la criticidad en cuanto a confidencialidad, y media en cuanto a integridad.

Por otra parte, dado que únicamente atiende a una parte de los usuarios de la red, se considera que la criticidad en cuanto a disponibilidad es media.

En el caso de la autenticidad y trazabilidad se le otorga una criticidad media.

• NEF: Criticidad media.

Este elemento es el responsable de garantizar la autenticación, confidencialidad e integridad de las comunicaciones de entidades externas al Núcleo de red, contra alguna de las funciones internas del Núcleo de red (interfaz *SBI*). Un acceso no autorizado, puede permitir la modificación de alguna política de seguridad entre las funciones externas al Núcleo de red y las internas. Sin embargo, esta función de red no se utiliza para la prestación de servicio generalista a los usuarios 5G. Por ese motivo, la confidencialidad e integridad tienen una valoración media.

Si atendemos a la disponibilidad, la caída de este equipo, en caso de no tener redundancia, sólo afectaría a aquellos servicios que necesiten comunicación externa con los elementos del Núcleo de red, lo que no tendría una afectación considerable y por eso se considera baja.

En el caso de la autenticidad y trazabilidad se le otorga una criticidad media.

– SMF/UPF y PCF: Criticidad baja.

Descripción del activo			Dimensión de Seguridad					Criticidad
Tipo	Dominio	Activo	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	
Primario	Núcleo de red	SMF/UPF	1 – Baja	1 – Baja	1 – Baja	1 – Baja	1 – Baja	1 – Baja
		PCF	1 – Baja	1 – Baja	1 – Baja	1 – Baja	1 – Baja	1 – Baja

En esta categoría se agrupan los siguientes elementos, en los que, en general, una afectación a los mismos no tiene un impacto notable en la prestación del servicio 5G, por lo que su valoración de criticidad es baja.

- SMF/UPF: Criticidad baja.

El SMF se encarga del establecimiento de las sesiones, y el UPF se encarga de la gestión del plano de usuario: desencapsula el tráfico del usuario que llega del acceso radio y lo encamina a otras redes de datos. Un acceso no autorizado puede desactivar la sesión de un usuario, pero se establecería en otro SMF/UPF. Además, el uso del SecGW entre la Red de acceso y el Núcleo de red imposibilita un MiTM, lo que hace que su criticidad atendiendo a la confidencialidad, integridad, autenticidad y trazabilidad sea baja.

Por otra parte, atendiendo a la disponibilidad, su criticidad se considera baja igualmente, debido a que un usuario no puede estar más que en un AMF, pero sus sesiones sí pueden estar en diversos SMF/UPF.

- PCF: Criticidad baja.

Este elemento no es especialmente crítico para los servicios de datos, siempre y cuando, además, los terminales sean de tipo data-centric. Aunque dispone de las políticas relacionadas con los servicios y la tarificación, los AMF/SMF siempre son configurados para poder dar servicio sin este elemento. Un efecto normal de caída de PCF en servicio de datos es no poder tarificar online a los clientes. La eventual afectación sobre el servicio de voz puede mitigarse mediante servicio de voz por 2G/3G. Por dichos motivos, su criticidad atendiendo a los diferentes criterios sería baja.

c) Transporte-Backhaul.

– SecGW: Criticidad alta.

Descripción del activo			Dimensión de Seguridad					Criticidad
Tipo	Dominio	Activo	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	
Primario	Transporte – Backhaul	SecGW	3 – Alta	2 – Media	2 – Media	2 – Media	2 – Media	3 – Alta

La red de transporte conecta los elementos del Núcleo con los de la Red de acceso. Un posible corte de esta en uno de sus tramos hace que solamente la zona de nodos de acceso radio en la que se produce dicho corte se vea afectada y, de forma temporal, se puede forzar a que el tráfico no pase por este elemento en dicha zona, con lo que la disponibilidad tiene una criticidad media.

Por otro lado, comprometer un sitio o interceptar el tráfico conlleva a una fuga de información importante, dado que es el elemento encargado de cifrar la información en tránsito que llega desde una gran cantidad de nodos. Por ello, atendiendo a la confidencialidad se le asigna una criticidad alta. Estando cifrada esta comunicación, alterarla es complicado, por lo que la criticidad en cuanto a integridad, autenticidad y trazabilidad se considera media.

d) Interconexión Roaming.

– SEPP: Criticidad alta.

Descripción del activo			Dimensión de Seguridad					Criticidad
Tipo	Dominio	Activo	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	
Primario	Interconexión Roaming	SEPP	3 – Alta	2 – Media	2 – Media	2 – Media	2 – Media	3 – Alta

Este elemento permite el intercambio de señalización con otras redes en escenarios de itinerancia. Pese a ser un elemento expuesto a otras redes, únicamente transporta tráfico de usuarios de *roaming*, y no el de los usuarios nacionales. Este hecho hace que la criticidad en cuanto a disponibilidad, autenticidad y trazabilidad sea media.

Por otra parte, la confidencialidad de las comunicaciones y su integridad sí son aspectos importantes (sobre todo la primera), pues es un entorno en el que, en caso de carecer de las protecciones adecuadas, se puede obtener o exfiltrar información sensible de los usuarios, incluso de aquellos que no están en *roaming*. Esto hace que la criticidad en cuanto a confidencialidad sea alta.

Es un entorno que la industria y los organismos de estandarización se ha tomado muy en serio, donde, de manera nativa, los fabricantes van a incluir capacidades de configuración de cifrado e integridad, lo que permite que, si el tráfico va cifrado, atentar contra la integridad sea más complicado, otorgándose una criticidad media.

e) Sistemas de control y gestión y servicios de soporte.

– GER: Criticidad alta.

Descripción del activo			Dimensión de Seguridad					Criticidad
Tipo	Dominio	Activo	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	
Primario	Sistemas de gestión/operación y servicios de soporte	GER	3 – Alta	3 – Alta	1 – Baja	3 – Alta	3 – Alta	3 – Alta

Estos elementos permiten una correcta operación de los elementos que conforman el entorno de red 5G. Pueden gestionar todo un entorno de red, intercambiando mensajes de configuración que pueden dar órdenes fraudulentas a los equipos, o incluso transportar credenciales.

Por tanto, se considera que la integridad, confidencialidad, autenticidad y trazabilidad de este elemento es alta.

Sin embargo, una interrupción o falta de comunicación con la red por parte de los Sistemas de gestión no ocasiona una caída de esta, considerando que la disponibilidad es de criticidad baja.

f) Infraestructura de virtualización /orquestación.

Descripción del activo			Dimensión de Seguridad					Criticidad
Tipo	Dominio	Activo	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	
Secundarios	Infraestructura de Virtualización/ Orquestación	Infraestructura de Virtualización	3 – Alta	3 – Alta	3 – Alta	3 – Alta	3 – Alta	3 – Alta
Secundarios		Gestión/Orquestación de Virtualización	3 – Alta	3 – Alta	1 – Baja	3 – Alta	3 – Alta	3 – Alta

– Infraestructura de virtualización: Criticidad alta.

Todos los elementos del Núcleo de red 5G se encuentran desplegados sobre una Infraestructura virtualizada. Esto implica que cualquier ataque que consiga una disrupción de su funcionamiento, poder controlar los nodos de esta, interceptar el tráfico, modificar el

funcionamiento, etc., puede tener graves consecuencias en la prestación del servicio, llegando a incluso su interrupción total. Por los motivos descritos, la criticidad en cuanto a confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad es alta, considerándose este un activo crítico dentro de la red.

– Gestión/orquestación de la virtualización: Criticidad alta.

De forma análoga a los Sistemas de gestión/operación y servicios de soporte, lo más crítico en este activo son la confidencialidad e integridad de las comunicaciones y accesos, calificadas de criticidad alta, pues desde los Orquestadores de la virtualización se controlan todos los elementos de la plataforma de virtualización, que podrían ser vulnerados o atentados (por ejemplo, eliminación de CNF, apagado de *hardware*, etc.). Así mismo se otorga a autenticidad y trazabilidad una criticidad alta.

Sin embargo, una interrupción o falta de comunicación con la red por parte del Orquestador no ocasiona una caída de las plataformas de virtualización, considerando así que la criticidad en cuanto a disponibilidad es baja.

g) Infraestructura física.

Descripción del activo			Dimensión de Seguridad					Criticidad
Tipo	Dominio	Activo	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	
Secundarios	Infraestructura Física	Infraestructura Física	1 – Baja	1 – Baja	3 – Alta	1 – Baja	1 – Baja	3 – Alta

– Infraestructura física: Criticidad alta.

La infraestructura física es especialmente vulnerable a los ataques que provocan daños físicos en el equipamiento, robo, cortes de energía, etc. La disponibilidad de esta es fundamental para el funcionamiento de las redes y los servicios, ya que se va a utilizar de base para ubicar muchas funciones de red y sistemas de gestión de toda la red, por lo que el valor de criticidad, en cuanto a disponibilidad, es alto.

La confidencialidad, integridad, autenticidad y trazabilidad de este activo se consideran bajas, dado que no representa un riesgo para la información o las comunicaciones en sí misma, dependiendo fundamentalmente de los protocolos y mecanismos de control lógicos implementados en las capas superiores (infraestructura de virtualización, aplicaciones, etc.), con objeto de evitar la obtención de información si alguien se hace con un activo.

Cuadro resumen: tabla de criticidad de activos

Descripción del activo			Dimensión de Seguridad					Criticidad
Tipo	Dominio	Activo	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad	
Primario	Red De Acceso	gNB	2 – Media	2 – Media	1 – Baja	2 – Media	2 – Media	2 – Media
Primario	Núcleo de red	SMF/UPF	1 – Baja	1 – Baja	1 – Baja	1 – Baja	1 – Baja	1 – Baja
		PCF	1 – Baja	1 – Baja	1 – Baja	1 – Baja	1 – Baja	1 – Baja
Primario	Núcleo de red	UDM	3 – Alta	3 – Alta	3 – Alta	3 – Alta	3 – Alta	3 – Alta
		UDR	3 – Alta	3 – Alta	3 – Alta	3 – Alta	3 – Alta	3 – Alta
		AUSF	3 – Alta	3 – Alta	3 – Alta	3 – Alta	3 – Alta	3 – Alta
Primario	Núcleo de red	AMF	3 – Alta	2 – Media	2 – Media	2 – Media	2 – Media	3 – Alta
		NRF	3 – Alta	3 – Alta	1 – Baja	3 – Alta	3 – Alta	3 – Alta
		NEF	2 – Media	2 – Media	1 – Baja	2 – Media	2 – Media	2 – Media
Primario	Transporte – Backhaul	SecGW	3 – Alta	2 – Media	2 – Media	2 – Media	2 – Media	3 – Alta
Primario	Interconexión Roaming	SEPP	3 – Alta	2 – Media	2 – Media	2 – Media	2 – Media	3 – Alta
Primario	Sistemas de gestión/operación y servicios de soporte	GER	3 – Alta	3 – Alta	1 – Baja	3 – Alta	3 – Alta	3 – Alta
Secundarios	Infraestructura de Virtualización/Orquestación	Infraestructura de Virtualización	3 – Alta	3 – Alta	3 – Alta	3 – Alta	3 – Alta	3 – Alta
Secundarios		Gestión/Orquestación de Virtualización	3 – Alta	3 – Alta	1 – Baja	3 – Alta	3 – Alta	3 – Alta
Secundarios	Infraestructura Física	Infraestructura Física	1 – Baja	1 – Baja	3 – Alta	1 – Baja	1 – Baja	3 – Alta

4. Clasificación de activos en función de la criticidad

En base a los análisis anteriores y a las aportaciones realizadas por los operadores de redes y servicios 5G, se ha identificado un conjunto de elementos calificándolos con importancia crítica para la operación de las redes 5G, para su configuración o gestión, o de los servicios prestados por las mismas.

Tal y como se ha recogido en el apartado anterior, todos los activos de criticidad alta del entorno primario de red pertenecen al Núcleo de red. No obstante, desde el punto de vista de la criticidad, no es posible considerar el Núcleo de red como un bloque homogéneo. Por ello, se considera aplicable un tratamiento diferenciado en relación a las medidas conducentes a garantizar la disponibilidad de los servicios que ofrecen.

Así pues, el Núcleo de red está compuesto de diversas funciones de red (o *Network Functions,* NF) que se despliegan en Infraestructuras virtualizadas independientes de la propia función de red. La clasificación considera cuáles de estas entidades son más críticas no sólo desde el punto de vista de redundancia, sino también del posible impacto de accesos no autorizados o ataques desde otras redes.

Además, se tiene en cuenta los posibles accesos no autorizados a la Infraestructura virtualizada sobre la que se despliegan estas funciones de red, y se establece una importancia relativa entre las distintas entidades, recalcando que, para obtener un servicio completo, todas ellas son necesarias.

a) Criticidad alta.

El riesgo que más comprometería el servicio 5G sería un acceso no autorizado al entorno AUSF/UDM/UDR. En el AUSF están las claves de autenticación que permiten el acceso a cualquier comunicación radio cifrada, y en el UDM/UDR se encuentran todos los datos de provisión de los usuarios y sus identidades, y precisamente el 3GPP ha incluido el uso del SUCI (identidad IMSI cifrada) para evitar que esa identidad viaje por el interfaz radio, ya que disponer del SUPI de un usuario es el primer paso para cualquier otro ataque. Se considera sin duda que estas son las funciones de red más críticas dado que el impacto de

obtener las claves y las entidades es duradero (al estar asociado a las claves de la SIM de los clientes). La pérdida de imagen de un operador de redes y servicios 5G ante una intrusión en estas funciones de red sería enorme y podría implicar la sustitución de las SIMs comprometidas. No obstante, el diseño de red permite proveer servicio sin ningún impacto ante fallo doble de instancias de cualquiera de estos nodos.

Además de los anteriores, se consideran de criticidad alta, entre otras, las siguientes funciones:

i. NRF: este elemento dispone de un mapa de toda la red, nodos y servicios. Con la información del NRF se dispone de todo el detalle del despliegue de la red, enrutamientos, DNNs, *slices,* servicios, etc. Además, un acceso no autorizado permitiría paralizar el servicio 5G ya que todas las funciones de red consultan a esta entidad para conocer las funciones de red destino que dispone del servicio requerido. No obstante, las funciones de red tienen cacheada la información de NRF, lo que permitiría mitigar temporalmente el ataque. A mayores, el diseño de red permite proveer el servicio sin ningún impacto ante fallo doble de instancias de este nodo.

ii. SEPP: permite el intercambio de señalización con otras redes para escenarios de itinerancia en la red propia, o en la de otras redes de terceros. Es un elemento expuesto, aunque los suministradores 5G han desarrollado un número elevado de funcionalidades para garantizar su seguridad e integridad. Adicionalmente, ha de garantizarse el aislamiento entre los dominios internos y externos.

iii. AMF: es el encargado de la gestión de la movilidad. Un ataque o acceso no autorizado al mismo, permitiría obtener información muy delicada (identidad del usuario, localización a nivel *Tracking Area,* e incluso gNB-id donde se encuentra el cliente cuando su terminal está en modo *connected)*, con posibilidad de rastrear el movimiento de usuarios, y sus procedimientos de señalización relacionados con la movilidad y gestión de sesiones. Estos elementos se despliegan en modo *pool* y se dimensionan para soportar de forma simultánea fallo de un nodo de cada *pool*.

b) Criticidad media.

En esta categoría de criticidad media se incluye la función NEF.

c) Criticidad baja.

En esta categoría, nuevamente, de mayor a menor criticidad, se indica:

i. SMF/UPF: SMF se encarga de la gestión de las sesiones (establecimiento, modificación y liberación), la gestión y asignación de IP a los terminales de los usuarios, etc. También es responsable de interactuar con el plano de usuario creando, actualizando o borrando sesiones PDU, así como de administrar el contexto de la sesión con el UPF, mientras que el UPF gestiona el plano de usuario. Estos elementos están mucho más redundados que los AMFs anteriormente descritos, y un acceso no autorizado podría desactivar la sesión de un usuario, aunque esta se establecería en otro SMF/UPF. El plano de usuario o tráfico real de clientes se encamina, en general a otras redes (internet/intranet) que son de seguridad más baja, por lo que un atacante de plano de usuario tiene más fácil comprometer el servicio atacando el servidor destino o incluso el terminal.

ii. PCF: no es especialmente crítico, ya que los AMF/SMF se configuran para poder dar servicio sin este elemento, afectando, eventualmente, a la tarificación online de los clientes.

d) No críticos.

Los elementos CHF, NWADF y 5G-EIR no se consideran críticos para prestación del servicio 5G debido a que, en caso de caída o indisponibilidad parcial o total de cualquiera de ellos, los clientes no deberían verse afectados en el servicio.

5. Identificación de amenazas y riegos en la tecnología 5G

En el artículo 9 del Real Decreto-ley 7/2022, de 29 de marzo, se especifica la necesidad de identificar los factores de riesgo a analizar en función de la evolución tecnológica, la incorporación de nuevos avances, funcionalidades y estándares tecnológicos, la situación

del mercado de comunicaciones electrónicas y del de suministros y de la aparición de nuevas amenazas y vulnerabilidades.

Los siguientes apartados recogen las tareas realizadas.

5.1 Criterio de identificación del riesgo de un ataque.

Para calcular el nivel de riesgo de seguridad que introduce una amenaza, utilizamos tres factores atendiendo a las siguientes fórmulas:

Nivel de riesgo = (Probabilidad de ocurrencia) × (Impacto en la red)

donde, a su vez,

(Impacto en la red) = (Criticidad del activo) × (Factor de escalado)

Se define, seguidamente, los conceptos empleados:

a) Probabilidad de ocurrencia: Se realiza una valoración en base a los siguientes parámetros:

i. Grado de exposición del activo a la vulnerabilidad: da una medida de lo expuesto que se encuentra el elemento analizado a nivel físico o lógico, y el nivel de accesibilidad/facilidad que pueda tener el atacante de cara a ejecutar la amenaza.

ii. Complejidad o conocimientos para desarrollar el ataque: la probabilidad de ocurrencia aumenta en el caso de que el ataque se pueda realizar sin muchos conocimientos técnicos y el entorno de ataque sea sencillo de implementar o se usen herramientas automatizadas.

iii. Conocimiento público de la vulnerabilidad: un ataque es más probable cuanto más conocido es a nivel de comunidad. En el caso de que la vulnerabilidad esté poco difundida o se maneje solamente en ciertos círculos (como por ejemplo suministradores 5G u operadores de redes y servicios 5G), su explotación será menos probable.

iv. Rastro que deja el ataque: en caso de que el ataque se realice por fuerza bruta o dejando trazabilidad en las redes, será menor la probabilidad de que existan atacantes dispuestos a aprovechar la vulnerabilidad. Se trata de casos en los cuales no pueda realizarse suplantación de identidad.

v. Beneficio obtenido con el éxito del ataque: valor económico, reconocimiento, relevancia, etc., de la consecución del ataque.

Los posibles valores de la probabilidad de ocurrencia son Muy Alto, Alto, Medio, Bajo.

b) Impacto en la red: de forma similar a la probabilidad de ocurrencia, se utiliza una valoración cualitativa para medir el impacto que podría tener el ataque en la red.

Para evaluar el servicio y dar una valoración del impacto se utilizan los siguientes parámetros:

i. Criticidad del activo: concepto mencionado anteriormente, que engloba la confidencialidad, la integridad, la disponibilidad, la autenticidad y la trazabilidad.

ii. Factor de escalado: identifica la importancia y/o alcance del ataque a nivel de afectación de la red. Toma en consideración tanto el alcance (número de usuarios que pueden ser impactados), como el tipo de impacto del ataque (fuga de credenciales, disminución de disponibilidad, etc.).

Los posibles valores del Impacto en red del ataque son: Muy Alto, Alto, Medio, Bajo, teniendo en cuenta los criterios anteriores.

c) Nivel de riesgo: Es el resultado de las dos variables anteriores siguiendo la fórmula descrita arriba.

Los posibles valores del nivel de riesgo son: Crítico, Alto, Medio, Bajo.

5.2 Matriz de riesgos.

Atendiendo a las consideraciones del apartado anterior, se presenta la matriz genérica que caracteriza los niveles de riesgo que se analizan posteriormente en este documento.

Impacto en la red	Baja (1)	Media (2)	Alta (3)	Muy Alta (4)
Muy Alto (4)	4	8	12	16
Alto (3)	3	6	9	12
Medio (2)	2	4	6	8
Bajo (1)	1	2	3	4

Probabilidad de ocurrencia

Nivel de riesgo
Crítico
Alto
Medio
Bajo

6. Amenazas o riesgos en una red 5G SA

Una vez identificados los activos y caracterizada su criticidad, el siguiente paso en el análisis de riesgos es evaluar las amenazas o posibles ataques a las que están expuestos cada uno de estos activos de red 5G SA.

Es importante destacar que una misma amenaza puede tener distinto nivel de riesgo en función del activo o entorno sobre el que se evalúe, de cara a establecer las prioridades correctas de acciones mitigadoras que permitan incrementar, en una misma línea temporal, la seguridad de la solución de la manera más eficiente posible.

A continuación, se detallan las amenazas o riesgos en una red 5G SA:

a) Actividades maliciosas debidas a accesos indebidos o maliciosos a la gestión, extracción de información sensible o modificación no autorizada de parametrización que provoque la indisponibilidad del elemento.

Se trata de aquellas acciones llevadas a cabo por atacantes internos o externos que van dirigidas a los elementos o funciones de red e infraestructura con la intención de robar información, alterarla o destruir, mediante configuración, un objetivo específico.

En este bloque se engloban, entre otras, las siguientes amenazas:

i. Intrusiones en la red con el objetivo de obtener información, a través de accesos maliciosos, movimientos laterales, escalado de privilegios, por falta de políticas de seguridad robustas (ausencia de control de acceso, autenticación, autorización, segmentación, *hardening,* etc). Destaca, entre otros la obtención de credenciales de usuarios operadores, información sensible de clientes (datos, identificadores de usuario, claves de autenticación, cifrado e integridad), o información útil de configuración de red (puertos, versiones, etc.), que sirva como vector de información adicional para realizar ataques de mayor impacto.

ii. Modificación malintencionada y no autorizada de parametrización o configuración de red que pueda provocar indisponibilidad parcial o total del servicio en el activo o la red, así como favorecer la exfiltración de tráfico comentada en el punto anterior.

A. Manipulación de configuración o parametrización que afecte al funcionamiento del equipo (políticas de enrutamiento de tráfico, configuración de DNS, sesiones de usuario, imágenes de funciones de red virtuales, etc.)

B. Manipulación de configuración de seguridad del equipo (políticas de seguridad, servicios ofrecidos en el aplicativo y sistema operativo, algoritmos criptográficos, reglas de acceso) y creación de puertas traseras.

C. Ejecución de forma intencionada o inconsciente de software/código malicioso (SQL, XSS injection, rootkits, malware/ransomware, etc.)

iii. Explotación de vulnerabilidades en *hardware* o *software*, que permitan un acceso simple y eficaz para poder ejecutar las amenazas comentadas en los dos puntos anteriores (vulnerabilidades conocidas/CVEs, nuevas vulnerabilidades y de zero-day).

b) Compromiso de las comunicaciones o datos de usuario a través de la captura, interceptación, secuestro de tráfico de servicio o su modificación:

Esta categoría recoge las acciones realizadas para espiar, interrumpir o alterar las comunicaciones o datos de usuario en el plano de servicio, sin su consentimiento.

Las principales amenazas dentro de esta categoría serían:

i. Espionaje de comunicaciones de un determinado usuario en entornos con alto nivel de exposición como es el caso del acceso radio o la interconexión de Roaming.

ii. Obtención de información sensible de los usuarios (identificadores de usuario, localización, servicios, etc) en interfaces expuestos que puedan ser utilizados como vectores de información para realizar ataques de mayor impacto.

iii. Manipulación de las comunicaciones en interfaces expuestos a través de actividades *Man in The Middle* (MiTM) y/o de los datos de usuario, siendo posible provocar acciones ilegales tales como fraude, suplantación de identidad, etc.

c) Denegación de Servicio (DoS).

Esta categoría recoge aquellas acciones, actividades o incidencias malintencionadas o no que puedan provocar una disrupción total o parcial en el equipo, causando una afectación a los usuarios de la red. Las principales amenazas dentro de esta categoría serían:

i. Ataques volumétricos de denegación de servicio (DoS/DDoS): Inundación de tráfico a las interfaces expuestas de los activos (dispositivos de usuario, interconexiones, etc.) buscando la sobrecarga de las capacidades de los elementos, con el objetivo de provocar un malfuncionamiento/disrupción en la red.

ii. Ataques dirigidos a usuarios específicos con el objetivo de provocar su indisponibilidad en la red (por ejemplo, ataques de interferencia o desregistro de la red).

iii. Daños no intencionados por los operadores por errores de configuración: Recoge las acciones no intencionadas por parte de un operador con acceso a la gestión de un activo que puedan resultar en un fallo o la reducción de funcionalidad de este, como, por ejemplo, la configuración pobre/errónea de los activos de red y sus capacidades de seguridad (aislamiento, bastionado, segmentación, etc.) o error en su gestión o manipulación por desconocimiento o falta de formación o diligencia.

iv. Mal funcionamiento del elemento: Engloba el malfuncionamiento «nativo» (por causas ajenas a la configuración del activo) que pueda provocar una disrupción total o parcial de su servicio.

d) Amenazas físicas.

Está dirigido a destruir, inutilizar, alterar o robar activos físicos de la infraestructura física que alberga la funciones/elementos de red.

Entre las amenazas principales destacan el sabotaje o terrorismo contra los elementos críticos de equipamiento de red, las catástrofes naturales, el malfuncionamiento de la red de energía y la posible sustracción de equipamiento de red para la extracción de información sensible y su posterior explotación.

e) Escasa formación y concienciación de los empleados en materia de ciberseguridad, así como mala praxis en la gestión de la evolución de los riesgos identificados.

Por un lado, el hecho de que los empleados no estén concienciados en materia de seguridad aumenta la probabilidad de ocurrencia de incidentes tales como ataques *ransomware* y otro tipo de *malware*. La falta de formación en materia de seguridad y operación aumenta la probabilidad de errores de configuración por desconocimiento que expongan los activos a riesgos innecesarios.

Además de todo esto, si no se lleva a cabo un buen procedimiento de gestión de riesgos, controlando su evolución en la red, será imposible plantear un plan de prioridades y ejecutar las medidas de seguridad de manera eficiente.

ANEXO III

Gestión de riesgos a nivel nacional

Una vez identificadas en el anexo II las distintas amenazas que afectan pormenorizadamente a las redes y servicios 5G, y con ello, la situación inicial de riesgo, la siguiente fase es prever aquellas medidas de seguridad necesarias para solventar, disminuir o paliar los riesgos identificados.

Estas medidas son:

1. Medidas de seguridad genéricas:

1.1 Configuraciones de seguridad para el equipamiento:

1.1.1 Configuraciones relacionadas con la identificación, autenticación, control, auditoría y monitorización en el acceso al plano de gestión de los nodos. Los nodos deben ser configurados con:

a) Políticas de gestión de identidad, permitiendo garantizar tanto la autenticación (verificar que quién accede es quién dice ser), como la autorización (acceder solo con los privilegios que sean estrictamente necesarios) cuando se accede a los nodos.
b) Políticas de gestión del ciclo de vida del usuario.
c) Capacidades de trazabilidad y políticas de auditoría, permitiendo que quede registrado todos los accesos (quién y cuándo se conecta y desconecta de los nodos), así como los comandos ejecutados y las alarmas que identifican un posible fallo en el equipo.
d) Buenas prácticas de seguridad cuando se definen y gestionan las credenciales y accesos de los usuarios, siempre forzando que las credenciales sean robustas.
e) Capacidad de ser configurados de tal manera que no den información detallada en el caso que falle el acceso y se establezcan políticas de bloqueo que dificulten la obtención de credenciales.

1.1.2 Bastionado:

a) Autoprotección de los nodos, asegurándose que solo estén activos los servicios necesarios para su correcto funcionamiento.
b) Los nodos deben tener la capacidad de separar el interfaz de gestión del de servicio, ya sea a través de un interfaz físico o lógico.
c) Los nodos deben ser capaces de detectar y manejar los paquetes malformados manteniendo los servicios sin afectación.
d) Los nodos deben ser capaces de hacer frente a altos volúmenes/picos de tráfico teniendo mecanismos de autorregulación para evitar el colapso de su CPU.
e) Capacidad adicional de proteger la información crítica y sensible que esté almacenada.
f) Los nodos/elementos de la red deben estar configurados de manera que no se permita iniciar a través de dispositivos de memoria no autorizados.
g) Los nodos deben configurarse de manera que no se pueda realizar una explotación maliciosa de las APIs que expongan.

1.1.3 Realización de pruebas de seguridad periódicas. Son necesarias para estudiar si han aparecido nuevas vulnerabilidades para los componentes del activo.

1.2 Seguridad de arquitectural y funcional.

1.2.1 Planos de red diferentes, así como áreas o ambientes de red con distinto nivel de exposición, deben ser aislados.
1.2.2 Control de flujo: Capacidad de limitar el tráfico a ciertas direcciones IPs, Protocolos, Aplicaciones, para evitar sobrecargar el enlace haciendo que un ataque sea más complicado de llevar a cabo.

1.3 Medidas de Seguridad en la Infraestructura Física:

a) Registro, validación y control de las autorizaciones de acceso físico a los emplazamientos críticos.
b) Controles de accesos físicos, mediante medios electrónicos y/o mecánicos, a las centrales de red y edificios relevantes.
c) Vigilancia física y seguridad electrónica del emplazamiento crítico.
d) Sistemas de seguridad electrónicos instalados y mantenidos en emplazamientos críticos.

1.4 Concienciación de seguridad hacia los empleados y la cadena de mando.
1.5 Formación de empleados en tecnología, seguridad y procesos.

1.6 Implementación de procesos claros de gestión de incidentes, teniendo un registro del histórico de incidentes propios y actualizado el conocimiento con los incidentes de la industria.

2. Medidas de seguridad específicas relacionadas con una red 5G.

2.1 Control de *software:*

a) Garantizar la integridad de la actualización del *software* antes de ser instalada, evitando la inyección de códigos maliciosos, troyanos o versiones no legítimas (manipuladas por un tercero).

b) Garantizar que no existan puertas traseras.

c) Garantizar que no existan vulnerabilidades (CVE) explotables conocidas de riesgo alto en el momento de despliegue del producto en planta.

d) Cumplimiento con certificaciones de seguridad reconocidas internacionalmente para los equipos.

2.2 Debe configurarse cifrado e integridad de las comunicaciones entre el terminal y la red a ambos niveles AS (Access Stratum)/NAS (Non Access Stratum), para proteger la privacidad del usuario en el interfaz aire. Esta medida se activa tanto en la RAN (AS), como en el Núcleo de Red (NAS).

2.3 Debe configurarse cifrado e integridad de las comunicaciones en el plano de control y en el plano de usuario entre el nodo de acceso radio (RAN) y el Núcleo de Red.

2.4 La privacidad de los usuarios debe ser garantizada en el interfaz aire.

2.5 Deben ser corroboradas las mejoras en los algoritmos de autenticación entre el terminal del usuario y la red que vienen de manera nativa con la tecnología 5G SA.

2.6 Mejoras nativas en los algoritmos de autenticación entre el dispositivo del usuario y la red, para garantizar mutuamente que la comunicación es legítima.

2.7 Los diferentes elementos que manejan el tráfico de señalización deben tener medidas para evitar la suplantación de los propios elementos de red en la red de *roaming,* así como la de los usuarios que no están en *roaming*.

2.8 La confidencialidad, integridad y autenticación deben ser garantizadas en las comunicaciones entre un operador origen y destino, usando protocolos/equipamiento/ soluciones seguras (SEPP). La implementación de este requisito y su alcance dependerá de la estandarización final del protocolo a utilizar.

2.9 Es necesario establecer las políticas de seguridad correspondientes de cara a exponer en la interconexión únicamente los interfaces y mensajes necesarios para el servicio, evitando dar información innecesaria que pueda ser utilizada de forma fraudulenta.

2.10 Aislamiento de funciones de red virtualizadas: Clasificación de los diferentes elementos virtualizados en la infraestructura de acuerdo con diferentes niveles de exposición y la criticidad del elemento.

2.11 Aislamiento de tráficos: Diseño seguro de la arquitectura de virtualización para garantizar el tráfico necesario para el funcionamiento de la capa de virtualización, de esta forma la operación/funcionamiento de la red será garantizado.

2.12 Es necesario seguir las pautas de los Requisitos/Configuraciones de Seguridad del Equipamiento y Seguridad Arquitectural para todos y cada uno de los elementos que componen la arquitectura de virtualización.

2.13 Monitorización y Detección: Monitorización de la trazabilidad de accesos y comandos ejecutados en los elementos críticos de la red, de cara a poder identificar actividades ilegítimas en el momento de su realización y también de cara al análisis forense de posibles ataques.

2.14 Mitigación: Capacidades que permitan mitigar posibles ataques volumétricos que tengan como objetivo la denegación de servicio en los interfaces muy expuestos.

2.15 Entornos críticos: Las pruebas de funcionamiento de redundancia/recuperación (backup) en entornos críticos deben llevarse a cabo antes del despliegue de la solución.

§ 47

Real Decreto 255/2025, de 1 de abril, por el que se regula el Documento Nacional de Identidad

Ministerio del Interior
«BOE» núm. 80, de 2 de abril de 2025
Última modificación: sin modificaciones
Referencia: BOE-A-2025-6601

El principio de seguridad jurídica es uno de los valores fundamentales sobre los que se articula el ordenamiento jurídico de un Estado de Derecho, quedando garantizado por nuestra Constitución de forma expresa en el apartado 3 del artículo 9.

El Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica, vino a unificar la dispersa normativa generada entonces, respecto a esta materia en diferentes disposiciones, lo que generaba disfunciones a la hora de su aplicación, derivadas tanto de la propia antigüedad de las normas, como de la dispersión de todas estas. Una vez más, con los continuos avances en las tecnologías y la normativa que lo regula, se hace preciso adaptarse a esta nueva situación.

El presente real decreto tiene como objeto la regulación del proceso de expedición, gestión y desarrollo del Documento Nacional de Identidad, en sus versiones física y digital, cuya finalidad es que la identidad de las personas debe establecerse dentro de un marco de seguridad jurídica que permita el reconocimiento y actuación de la ciudadanía de manera individual, y garantice la protección de sus derechos, desarrollando mecanismos de identificación y autenticación que proporcionen seguridad en sus relaciones con el sector público y privado.

En este contexto, la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana, y, en concreto, en su artículo 8.1, regula expresamente la naturaleza jurídica del Documento Nacional de Identidad como documento público y oficial, que tendrá la protección que a estos otorgan las leyes. Es el único documento con suficiente valor por sí solo para la acreditación, a todos los efectos, de la identidad y los datos personales de su titular.

De igual forma, se establece en sus artículos 9 y 16 que todas las personas obligadas a obtener el Documento Nacional de Identidad lo están también a exhibirlo y permitir la comprobación de las medidas de seguridad por la autoridad y sus agentes con la finalidad de identificación de las personas.

A los efectos de lo dispuesto en el marco legal, este real decreto cumple las obligaciones establecidas para que la ciudadanía pueda disponer de su Documento Nacional de Identidad, a efectos de identificación, con su formato físico o formato digital a través de una comunicación segura por medio de una aplicación en un dispositivo móvil, sin que se comprometa la seguridad jurídica de la identidad segura que la legislación vigente atribuye al Documento Nacional de Identidad.

Otra cuestión importante que se introduce en este real decreto es la adaptación del Documento Nacional de Identidad al Reglamento (UE) 2019/1157 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, sobre el refuerzo de la seguridad de los documentos de identidad de los ciudadanos de la Unión y de los documentos de residencia expedidos a ciudadanos de la Unión y a los miembros de sus familias que ejerzan su derecho a la libre circulación.

El propio Reglamento (UE) 2019/1157 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, establece unas características técnicas de almacenamiento, como ya se contempla para los pasaportes y los permisos de residencia para ciudadanos de terceros países. Es un método apropiado para combinar una identificación y una autenticación fiables con un riesgo reducido de fraude, con el fin de abordar adecuadamente el objetivo de reforzar la seguridad de los documentos de identidad y las tarjetas de residencia.

El Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE, refuerza la confianza en este tipo de transacciones. Con la entrada en vigor del Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento (UE) 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital, se establece un marco jurídico para las firmas electrónicas, los sellos electrónicos, los sellos de tiempo electrónicos, los documentos electrónicos, los servicios de entrega electrónica certificada, los servicios de expedición de certificados para la autenticación de sitios web, el archivo electrónico, la declaración electrónica de atributos, la gestión de dispositivos de creación de firma electrónica a distancia o dispositivos de creación de sello electrónico a distancia y los libros mayores electrónicos.

En el marco del espacio digital homogéneo de la Unión Europea, y conforme a la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, introduce el sello electrónico de persona jurídica, el servicio de validación de firmas y sellos cualificados, su conservación, el sellado electrónico de tiempo, su entrega certificada y certificados de autenticación web, que pueden ser combinados entre sí para la prestación de servicios complejos e innovadores, permitiendo al Documento Nacional de Identidad ser el identificador único vinculado a la generación de identidad en los certificados cualificados y atributos para nuevas funcionalidades, como su versión digital que se integran en una infraestructura de datos de alta calidad, conectividad y ciberseguridad europea.

La Ley 6/2021, de 28 de abril, por la que se modifica la Ley 20/2011, de 21 de julio, del Registro Civil, consolida la implantación de un nuevo modelo de Registro Civil único para toda España, que precisa necesariamente de un periodo de implementación desde el punto de vista tecnológico, estructural y organizativo, donde forma parte esencial la asignación del Documento Nacional de Identidad a las personas inscritas en el Registro Civil.

En el ámbito de la protección de datos, este real decreto se articula en conformidad con lo previsto en el Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos) y en la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales, o en su caso, la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y la ejecución de sanciones penales, el resto de normativa de aplicación, así como los criterios que se establezcan por la Agencia Española de Protección de Datos.

El objetivo que se pretende es regular en un mismo instrumento normativo de aplicación directa, la expedición del Documento Nacional de Identidad, su gestión y transformación digital, para cubrir aquellos aspectos previstos en el desarrollo legislativo, con la intención de garantizar el acceso de toda la ciudadanía en la obtención del Documento Nacional de Identidad, y su adaptación en la usabilidad de los nuevos retos digitales, siendo la expedición del Documento Nacional de Identidad condición necesaria, para la obtención en formato digital.

Este real decreto se ajusta a los principios de buena regulación contenidos en el artículo 129 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. Se adecúa a los principios de necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia y eficiencia, que contribuyen a dotar de mayor seguridad jurídica, cumplir con el principio de transparencia e identificar su propósito.

La necesidad de que las personas se identifiquen por medios electrónicos con las administraciones públicas y el sector privado, simplificando el acceso a los mismos, debe ser proporcional al refuerzo en el empleo de las tecnologías de la información y las comunicaciones, tanto para mejorar la eficiencia de su gestión como para potenciar y favorecer las relaciones de colaboración y cooperación entre ellas.

Asimismo, esta necesidad consiste en incrementar la transparencia de la identificación y facilitar la participación de las personas en la administración electrónica del sector público y privado.

De igual forma, persigue garantizar un servicio de identificación fácilmente utilizable de modo que se pueda conseguir que la relación de la ciudadanía con la Administración sea fácil, intuitiva y efectiva cuando use el Documento Nacional de Identidad, en cualquiera de sus formatos, físico, electrónico o digital.

Por último, busca mejorar la seguridad jurídica, para garantizar a todas las personas intervinientes que sirva a los objetivos de mejorar la eficiencia administrativa para hacer efectiva una identificación totalmente electrónica o digital y garantizar a la ciudadanía servicios digitales fácilmente utilizables con una identificación con el Documento Nacional de Identidad de forma segura, en consonancia con el resto del ordenamiento jurídico nacional y de la Unión Europea.

El real decreto se dicta en ejercicio de la habilitación normativa contenida en la disposición final cuarta de la Ley Orgánica 4/2015, de 30 de marzo, y en la disposición final sexta de la Ley 6/2020, de 11 de noviembre, para llevar a cabo su desarrollo reglamentario en lo referido a la regulación y tramitación del Documento Nacional de Identidad, tratamiento de los datos de identidad y sus aspectos digitales, así como la efectiva aplicación e implantación de las previsiones que ambas leyes establecen. Todo ello al amparo de lo dispuesto en el artículo 149.1.8.ª, 18.ª, 21.ª y 29.ª de la Constitución, que atribuye al Estado la competencia exclusiva en materia de legislación civil, bases del régimen jurídico de las administraciones públicas, telecomunicaciones y seguridad pública.

En su virtud, a propuesta del Ministro del Interior, con la aprobación previa del Ministro para la Transformación Digital y de la Función Pública, de acuerdo con el Consejo de Estado, y previa deliberación del Consejo de Ministros en su reunión del día 1 de abril de 2025,

DISPONGO:

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

Este real decreto tiene como objeto la regulación del proceso de expedición, gestión y desarrollo del Documento Nacional de Identidad, en sus versiones física y digital.

Artículo 2. *Naturaleza y funciones.*

1. El Documento Nacional de Identidad es un documento personal e intransferible emitido por el Ministerio del Interior, a través de la Dirección General de la Policía, que goza de la protección que a los documentos públicos y oficiales otorgan las leyes.

2. A cada Documento Nacional de Identidad se le asignará un número personal que tendrá la consideración de identificador numérico personal de carácter general.

3. El Documento Nacional de Identidad consiste en una tarjeta inteligente certificada que permite a la ciudadanía la identificación física mediante la exhibición del documento y la identificación digital, por un procedimiento seguro a través de un dispositivo móvil para

acreditar electrónicamente la identidad de las personas, ya sea de manera presencial o remota.

Artículo 3. *Fines.*

1. El Documento Nacional de Identidad es el único documento con suficiente valor por sí solo para la acreditación, a todos los efectos, de la identidad y los datos personales de su titular. Permite la identificación electrónica de su titular, así como la firma electrónica de documentos, en los términos previstos en la legislación específica.
2. Todas las personas físicas o jurídicas, públicas o privadas, reconocerán la eficacia del Documento Nacional de Identidad, a los efectos de acreditar la identidad y los demás datos personales del titular que consten en el mismo, así como su firma y la integridad de los documentos firmados con sus certificados electrónicos.

CAPÍTULO II

Sobre derechos, obligaciones y órganos competentes

Artículo 4. *Derechos y obligaciones.*

1. Todas las personas con nacionalidad española tienen derecho a que se les expida el Documento Nacional de Identidad.
2. Su obtención es obligatoria para las personas mayores de catorce años residentes en España y para las de igual edad que, residiendo en el extranjero, se trasladen a España por tiempo no inferior a seis meses.
3. El Documento Nacional de Identidad es personal e intransferible, debiendo su titular mantenerlo en vigor, conservarlo y custodiarlo con la debida diligencia.
4. Ninguna persona con nacionalidad española podrá ser privada del Documento Nacional de Identidad, ni siquiera temporalmente, salvo en los casos y forma establecidos por las leyes, en los que haya de ser sustituido por otro documento.
5. Todas las personas obligadas a obtener el Documento Nacional de Identidad lo están también a exhibirlo cuando fueren requeridas para ello por la autoridad, sus agentes y funcionarios públicos en el desempeño de sus funciones, para permitir comprobar los datos contenidos en él, independientemente de su formato físico o digital, así como las condiciones de calidad e inalterabilidad del mismo. De su sustracción o extravío deberá darse cuenta, tan pronto como sea posible, a la comisaría de Policía o puesto de las Fuerzas y Cuerpos de Seguridad más próximo. La denuncia policial o administrativa, será requisito necesario en la obtención de un duplicado, de conformidad con lo expuesto en el artículo 9.1.

Artículo 5. *Órgano competente para la tramitación.*

1. Corresponde al Ministerio del Interior la competencia exclusiva para la dirección, organización, desarrollo, administración y gestión de todos los aspectos referentes al Documento Nacional de Identidad.
2. Dicha competencia será ejercida por la Dirección General de la Policía, gestionando la custodia y responsabilidad de la actividad del tratamiento de los datos personales en conformidad con la legislación en materia de protección de datos.

CAPÍTULO III

Sobre tramitación, expedición, validez y renovación

Artículo 6. *Tramitación y requisitos.*

1. El Documento Nacional de Identidad se tramitará, en su formato físico y digital, conforme a la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. El Ministro de Interior, a través de la Dirección General de la Policía, recibirá la asistencia y colaboración requerida para su cumplimiento.
2. En este proceso se cumplirán los siguientes requisitos:

a) La tramitación del Documento Nacional de Identidad se realizará con la presencia física de la persona, a través de los sistemas de cita previa, en atención a los recursos humanos y materiales disponibles, igualmente, se podrá expedir con carácter excepcional sin cita previa, así como en colaboración con otras Administraciones Estatales, Autonómicas o Locales.

b) En caso de menores de edad, se llevará a cabo en presencia de quien tenga encomendada la patria potestad o tutela, medida de apoyo, o persona apoderada por estas últimas.

c) La expedición o cualquier otro trámite relacionado con el Documento Nacional de Identidad conllevará el abono de la tasa legalmente establecida, sin perjuicio de las exenciones de tasas establecidas en conformidad con la legislación vigente.

d) Los documentos necesarios para la expedición del Documento Nacional de Identidad por primera vez, serán recabados electrónicamente, salvo que la persona interesada se opusiera a ello. Excepcionalmente, si las administraciones públicas no pudieran recabar los citados documentos, podrán solicitar nuevamente al interesado su aportación.

Los documentos necesarios para la expedición son los siguientes:

1.º El documento acreditativo del Registro Individual de la persona que solicita el documento.

Se consultará por la Dirección General de Policía, por medios electrónicos, la base de datos del Registro Civil, de conformidad con lo establecido en la Ley 20/2011, de 21 de julio, del Registro Civil, y la Ley 6/2021, de 28 de abril, por la que se modifica la Ley 20/2011, de 21 de julio, del Registro Civil, a los efectos de obtención del Registro Individual de la persona que solicita el documento de los datos necesarios para la expedición del Documento Nacional de Identidad.

2.º Certificado o volante de empadronamiento del Ayuntamiento donde la persona solicitante tenga su domicilio, expedido con una antelación máxima de tres meses a la fecha de la tramitación del Documento Nacional de Identidad.

3.º Las personas con nacionalidad española residentes en el extranjero acreditarán el domicilio mediante certificación de la Representación Diplomática o Consular donde estén inscritos como residentes, expedida con una antelación máxima de tres meses a la fecha de la tramitación del Documento Nacional de Identidad.

4.º Una fotografía reciente del rostro de la persona solicitante en color, tamaño 32 por 26 milímetros, con fondo uniforme blanco y liso, tomada de frente, con la cabeza totalmente descubierta y sin gafas de cristales oscuros o cualquier otra prenda que pueda impedir o dificultar la identificación de la persona. Dicha fotografía podrá ser realizada de forma automatizada en aquellas Unidades de Documentación dotadas de ese recurso técnico.

e) Excepcionalmente, en los supuestos en los que, por circunstancias ajenas a la persona solicitante, no pudiera ser presentado alguno de los documentos necesarios o recabados electrónicamente, y siempre que los datos que consten en tales documentos se acrediten por otros medios, suficientes a juicio de la persona responsable de la Unidad encargada de la expedición, esta, estará facultada para expedir un Documento Nacional de Identidad con validez restringida, de conformidad con lo expuesto en el artículo 7.2.b).

f) El Documento Nacional de Identidad incluirá un medio de almacenamiento de alta seguridad que contendrá una imagen facial del titular del documento. Igualmente, se incluirán dos impresiones dactilares en formatos digitales interoperables, a excepción de los menores de seis años. Se tomarán las impresiones dactilares de los dedos índices de ambas manos a la persona interesada. Si no fuere posible obtener la impresión dactilar de alguno de los dedos o de ambos, se sustituirá, en relación con la mano que corresponda, por otro dedo según el siguiente orden de prelación: medio, anular o pulgar; consignándose, en el lugar del soporte destinado a tal fin, el dedo utilizado, o la imposibilidad de obtener alguno de ellos. Las personas a las que sea físicamente imposible quedarán exentas del requisito de facilitarlas.

g) Se recogerá igualmente, la firma manuscrita digitalizada que constará al menos de alguno de los siguientes elementos, nombre, apellidos, letras contenidas en estos y la rúbrica. Quedan excluidas las firmas que reflejen dibujos, pictogramas, figuras, caricaturas,

acrónimos, leyendas o cualquier elemento que no guarde relación con su identidad, con los datos que figuren en el DNI ni sirvan para su identificación.

Artículo 7. *Validez.*

1. Con carácter general el Documento Nacional de Identidad tendrá un período de validez, a contar desde la fecha de la expedición o de cada una de sus renovaciones, de:

a) Dos años cuando la persona titular no haya cumplido los cinco años de edad.
b) Cinco años, cuando la persona titular haya cumplido los cinco años de edad y no haya alcanzado los treinta al momento de la expedición o renovación.
c) Diez años, cuando la persona titular haya cumplido los treinta y no haya alcanzado los setenta.
d) Más de diez años cuando la persona titular haya cumplido los setenta años, consignando una fecha.

2. De forma excepcional se podrá otorgar validez de un año al Documento Nacional de Identidad en los siguientes supuestos de expedición y renovación:

a) Cuando sea físicamente imposible, con carácter temporal, tomar las impresiones dactilares de cualquier dedo de la persona solicitante.
b) En los supuestos del artículo 6.2.e), una vez aportada y verificada la documentación necesaria se le modificará la validez a la vigencia correspondiente según su edad.

Artículo 8. *Renovación.*

1. Transcurrido el período de validez del Documento Nacional de Identidad se considerará caducado, revocándose las atribuciones y efectos que le reconoce el ordenamiento jurídico. Su titular estará obligado a proceder a su renovación.
2. La renovación del Documento Nacional de Identidad podrá tramitarse dentro de los últimos 180 días de su vigencia. Se llevará a cabo mediante la presencia física de la persona titular del documento, que deberá abonar la tasa correspondiente, sin perjuicio de las exenciones establecidas, y aportar una fotografía con las características señaladas en el artículo 6.2.d). También se le recogerán las impresiones dactilares que se refieren en el párrafo f) del mismo artículo.
3. También se deberá proceder a la renovación del Documento Nacional de Identidad en los supuestos de variación de los datos que se recogen en el mismo, en cuyo caso será preciso recabar los documentos justificativos que acrediten dicha variación.

Artículo 9. *Expedición de duplicados.*

1. El extravío, sustracción, destrucción o deterioro del Documento Nacional de Identidad, conllevará la obligación de su titular de proveerse inmediatamente de un duplicado, que será expedido de forma que se garantice la seguridad jurídica del titular, debiendo presentar denuncia policial o administrativa en caso de extravío y sustracción. La validez de estos duplicados será la misma que tenían los documentos de identidad a los que sustituyen, salvo que estos se hallen dentro de los últimos 90 días de su vigencia, en cuyo caso se expedirán con la misma validez que si se tratara de una renovación.
2. Los documentos sustituidos perderán el carácter de Documento Nacional de Identidad, así como los efectos que el ordenamiento jurídico atribuye a este con respecto a su titular.

Artículo 10. *Entrega del Documento Nacional de Identidad.*

La entrega del Documento Nacional de Identidad deberá realizarse personalmente a su titular. Cuando la persona titular sea menor de 14 años o una persona con una medida de apoyo para el pleno ejercicio de su capacidad jurídica, el acto de entrega se llevará a cabo a quien tenga encomendada la patria potestad, tutela, medida de apoyo, o persona apoderada por estas últimas.

Artículo 11. *Características de la tarjeta soporte.*

1. El material, formato y diseño de la tarjeta soporte del Documento Nacional de Identidad se determinará por orden de la persona titular del Ministerio del Interior, teniendo en cuenta en su elaboración la utilización de procedimientos y productos tendentes a la consecución de condiciones de calidad, inalterabilidad y máximas garantías para impedir su falsificación y manipulaciones fraudulentas de que pueda ser objeto, conforme al Reglamento (UE) 2019/1157 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, sobre el refuerzo de la seguridad de los documentos de identidad de los ciudadanos de la Unión y de los documentos de residencia expedidos a los ciudadanos de la Unión y a sus familiares que ejercen su derecho a la libre circulación.

2. La tarjeta soporte contiene un chip, como medio de almacenamiento de alta seguridad, donde se integran de forma separada:

a) Los certificados electrónicos cualificados que funcionan con un dispositivo cualificado de creación de firma electrónica, conforme al Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, modificado por el Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, y de acuerdo con la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, garantizando la identidad del titular de la clave privada de identificación y firma, permitiendo la generación de la firma electrónica avanzada y cualificada. El Ministerio para la Transformación Digital y de la Función Pública, será el órgano de supervisión del cumplimiento de las obligaciones establecidas a la Dirección General de la Policía.

b) La fotografía, los datos personales del titular del documento y las dos impresiones dactilares en formatos digitales interoperables.

3. El plazo de validez de los certificados electrónicos contenidos en el Documento Nacional de Identidad será de dos años.

4. El Ministro de Interior, a través de la Dirección General de la Policía, formulará una Declaración de Prácticas y Políticas de Certificación, que podrán ser consultadas de manera pública en la web de la Policía Nacional, de conformidad con la legislación vigente en materia de accesibilidad universal.

Artículo 12. *Contenido del Documento Nacional de Identidad.*

El Documento Nacional de Identidad, además de lo específicamente dispuesto por el Reglamento (UE) 2019/1157 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, contendrá la siguiente información:

a) En el anverso:

Número y carácter de verificación personal e intransferible del Documento Nacional de Identidad.
Apellidos y nombre.
Fecha de nacimiento.
Sexo.
Nacionalidad.
Emisión del documento.
Validez.
Número de soporte.
Fotografía digitalizada.
Firma manuscrita digitalizada.

b) En el reverso:

Domicilio.
Lugar de nacimiento.
Nombre de los progenitores.
Número de Equipo de la Unidad de Documentación.
Tres líneas MRZ que contienen 30 caracteres OCR-B cada una.
Chip electrónico.

CAPÍTULO IV

Sobre las especificidades de la versión digital del Documento Nacional de Identidad

Artículo 13. *Versión digital del Documento Nacional de Identidad.*

1. El Ministerio del Interior, a través de la Dirección General de la Policía, será el responsable de la versión digital del Documento Nacional de Identidad, que se realizará a través de una infraestructura de identificación electrónica con un dispositivo móvil.

2. La Dirección General de la Policía establecerá una actuación administrativa automatizada para la obtención de la versión digital del Documento Nacional de Identidad, de manera electrónica, telemática o presencial, teniendo de forma alternativa la misma finalidad que el formato físico para la identificación de las personas.

3. El Documento Nacional de Identidad en su versión digital se generará siempre que la persona titular disponga de su documento físico vigente. Permitirá tener acceso a sus datos personales, usarlos y gestionarlos de forma segura, independientemente de su ubicación. La versión digital tendrá los mismos plazos de validez que la versión física, indicados en el artículo 7.

4. La utilización del Documento Nacional de Identidad en su versión digital tendrá la misma eficacia jurídica a efectos de identificación. Permitirá acreditar la identidad ante las autoridades, sus agentes y funcionarios públicos, así como en las relaciones con las Administraciones Públicas y con el sector privado.

5. El funcionamiento de la versión digital consiste en virtualizar el Documento Nacional de Identidad en el dispositivo móvil, a través de una comunicación segura, sin que se comprometa la garantía de la identidad segura que la legislación vigente atribuye al Documento Nacional de Identidad.

CAPÍTULO V

Sobre la protección en el tratamiento de los datos personales

Artículo 14. *Tratamiento de los datos personales.*

1. Al tratamiento de los datos personales del Documento Nacional de Identidad le será de aplicación lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecto al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos) y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, o en su caso, la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y la ejecución de sanciones penales, el resto de normativa de aplicación, así como los criterios que se establezcan por la Agencia Española de Protección de Datos.

Disposición adicional primera. *Documento de sustitución del Documento Nacional de Identidad en supuestos de retirada.*

En los supuestos en que, de acuerdo con las previsiones establecidas en las leyes, sea acordada por la autoridad competente la retirada temporal de Documento Nacional de Identidad por los órganos encargados de su expedición, se facilitará a la persona interesada un documento identificador que tendrá las características y funcionalidades que determine el Ministerio del Interior, atendiendo a las causas de su retirada.

Disposición adicional segunda. *Documento Nacional de Identidad de las personas menores de edad.*

La posesión del Documento Nacional de Identidad por menores de edad no supone, por sí sola, autorización para desplazarse fuera del territorio nacional, debiendo ser suplida, a estos efectos, con la correspondiente autorización de quien ejerza la patria potestad o tutela.

Disposición adicional tercera. *Imposibilidad de expedición o renovación del Documento Nacional de Identidad.*

Cuando exista imposibilidad manifiesta para la expedición del Documento Nacional de Identidad, y sin perjuicio de que por las autoridades y órganos correspondientes se compruebe la identidad del interesado por cualesquiera otros medios, excepcionalmente podrá sustituirse aquél por certificaciones anuales en las que consten los motivos de tal imposibilidad, que en los supuestos de renovación tendrán únicamente el fin de prorrogar la validez del documento caducado.

Disposición adicional cuarta. *Expedición del Documento Nacional de Identidad en el exterior.*

Las personas con nacionalidad española que se encuentren en el exterior podrán solicitar que se les expida el Documento Nacional de Identidad en las embajadas y consulados en los que la Dirección General de la Policía cuente con los recursos técnicos y humanos necesarios para su expedición. Las condiciones en las que la Dirección General de la Policía prestará este servicio se establecerán previo acuerdo del Ministerio del Interior con el Ministerio de Asuntos Exteriores, Unión Europea y Cooperación.

Disposición transitoria primera. *Validez de los Documentos Nacionales de Identidad expedidos con anterioridad a la entrada en vigor de este real decreto.*

Los Documentos Nacionales de Identidad emitidos con anterioridad a la entrada en vigor de este real decreto seguirán siendo válidos y eficaces, de conformidad con la normativa aplicable en el momento de su expedición o renovación.

Disposición transitoria segunda. *Medidas hasta la implantación de la Ley 20/2011, de 21 de julio, del Registro Civil.*

Mientras no esté implantada la Ley 6/2021, de 28 de abril, por la que se modifica la Ley 20/2011, de 21 de julio, del Registro Civil, en todo el territorio nacional, las personas que no dispongan de Registro individual deberán aportar certificación literal de nacimiento, en la que conste la anotación de que se ha emitido a los solos efectos de la obtención del Documento Nacional de Identidad y siempre que se hayan expedido con una antelación máxima de seis meses a la fecha de la tramitación del documento.

Disposición transitoria tercera. *Adaptación de las entidades a la versión digital del Documento Nacional de Identidad.*

Las entidades pertenecientes al sector público y privado deberán adoptar en el plazo de doce meses desde la entrada en vigor de este real decreto, las medidas necesarias para el buen funcionamiento de la versión digital del Documento Nacional de Identidad.

Disposición derogatoria única. *Derogación normativa.*

1. Queda derogado el Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica.
2. Asimismo, quedan derogadas todas aquellas normas de igual o inferior rango que se opongan a lo preceptuado en este real decreto.

Disposición final primera. *Modificación del Real Decreto 991/2024, de 1 de octubre, sobre inscripción de las personas de nacionalidad española en los Registros de Matrícula de las Oficinas Consulares en el extranjero.*

El Real Decreto 991/2024, de 1 de octubre, sobre inscripción de las personas de nacionalidad española en los Registros de Matrícula de las Oficinas Consulares en el extranjero, queda modificado como sigue:

Uno. El apartado 5 del artículo 1 queda redactado en los siguientes términos:

«5. El Registro de Matrícula Consular otorgará a cada persona inscrita, residente o no residente, un Número de Identificación Consular Central, previa consulta a la Dirección General de la Policía del Ministerio del Interior, que será un código o número identificativo único y permanente. Dicho número tendrá el mismo formato del número utilizado por el Documento Nacional de Identidad (DNI). Se basará en el número del DNI, para aquellas personas que ya lo posean, o, en caso contrario, se extraerá del Código Personal de la inscripción realizada en el Registro Civil proporcionado por DICIREG.

Podrá asignarse, sin embargo, un número identificativo de carácter temporal a aquellas personas de nacionalidad española de las que no se tengan registros biométricos asociados a su identidad o si fuera necesario durante el periodo de implantación del nuevo modelo de Registro. Una vez se compruebe la identidad de dichas personas a través de nuevos registros biométricos o termine el proceso de implantación se les otorgará el Número de Identificación Consular Central permanente mencionado.

El Número de Identificación Consular Central no tendrá ningún valor identificativo por sí solo.»

Dos. El apartado 4 del artículo 2 queda redactado en los siguientes términos:

«4. Para el acceso a los servicios del Registro de Matrícula Consular ofrecidos en la sede electrónica asociada de la Administración General del Estado del Ministerio de Asuntos Exteriores, Unión Europea y Cooperación, las personas de nacionalidad española que se encuentren en el exterior podrán emplear como medios de identificación cualesquiera de los establecidos en el artículo 9 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, en la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza y en la sección 3.ª del capítulo II del título II del Reglamento de actuación y funcionamiento del sector público por medios electrónicos, relativa a la identificación y firma de las personas interesadas, aprobado por el Real Decreto 203/2021, de 30 de marzo, así como cualquier otro sistema adicional que pueda desarrollarse y que cumpla lo establecido en la normativa vigente.

El Ministerio de Asuntos Exteriores, Unión Europea y Cooperación habilitará una Autoridad de Certificación Consular que permitirá otorgar certificados electrónicos cualificados a las personas de nacionalidad española, residentes en el exterior que no posean un DNI en vigor. El Número de Identificación Consular Central permanente será equivalente al número del DNI para la emisión de dichos certificados digitales cualificados, que permitirán identificarse ante las diferentes administraciones públicas.»

Disposición final segunda. *Modificación del Reglamento de actuación y funcionamiento del sector público por medios electrónicos, aprobado por el Real Decreto 203/2021, de 30 de marzo.*

El Reglamento de actuación y funcionamiento del sector público por medios electrónicos, aprobado por el Real Decreto 203/2021, de 30 de marzo, queda modificado como sigue:

Uno. El apartado 1 del artículo 27 queda redactado del siguiente modo:

«1. Los sistemas basados en certificados cualificados de firma electrónica admitidos por las Administraciones Públicas para la identificación electrónica de persona física a que se refiere el artículo 9.2.a) de la Ley 39/2015, de 1 de octubre,

emitidos al amparo de la Ley 6/2020, de 11 de noviembre, deberán contener como atributos, al menos, su nombre y apellidos y su número de Documento Nacional de Identidad, Número de Identificación de Extranjero, Número de Identificación Consular Central o Número de Identificación Fiscal que conste como tal de manera inequívoca. La comprobación de la identidad y otras circunstancias de los solicitantes del certificado se realizará de conformidad con lo previsto en el artículo 7 de la Ley 6/2020, de 11 de noviembre.»

Dos. El apartado 1 del artículo 28 queda redactado del siguiente modo:

«1. Los sistemas de clave concertada o cualquier otro sistema que las Administraciones Públicas consideren válidos, admitidos para la identificación electrónica de persona física de conformidad con el artículo 9.2.c) de la Ley 39/2015, de 1 de octubre, deberán ajustarse a lo previsto en el Esquema Nacional de Seguridad y contener, como mínimo, el nombre y apellidos y el número de Documento Nacional de Identidad, Número de Identificación de Extranjero, Número de Identificación Consular Central o Número de Identificación Fiscal y, para los casos en que así se establezca en la definición del sistema, el número de pasaporte.»

Disposición final tercera. *Título competencial.*

Este real decreto se dicta al amparo de lo dispuesto en el artículo 149.1.8.ª, 18.ª, 21.ª y 29.ª de la Constitución, que atribuye al Estado la competencia exclusiva en materia de legislación civil, bases del régimen jurídico de las administraciones públicas, telecomunicaciones y seguridad pública.

Disposición final cuarta. *Desarrollo normativo.*

Se habilita a la persona titular del Ministerio del Interior para que dicte, en el ámbito de sus competencias, cuantas disposiciones sean necesarias para el desarrollo y aplicación de este real decreto.

Disposición final quinta. *Entrada en vigor.*

El presente real decreto entrará en vigor el mismo día de su publicación en el «Boletín Oficial del Estado».

§ 48

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 281, de 24 de noviembre de 1995
Última modificación: 11 de junio de 2024
Referencia: BOE-A-1995-25444

[. . .]

LIBRO I

Disposiciones generales sobre los delitos, las personas responsables, las penas, medidas de seguridad y demás consecuencias de la infracción penal.

[. . .]

TÍTULO II

De las personas criminalmente responsables de los delitos

Artículo 27.

Son responsables criminalmente de los delitos los autores y los cómplices.

Artículo 28.

Son autores quienes realizan el hecho por sí solos, conjuntamente o por medio de otro del que se sirven como instrumento.

También serán considerados autores:

a) Los que inducen directamente a otro u otros a ejecutarlo.

b) Los que cooperan a su ejecución con un acto sin el cual no se habría efectuado.

Artículo 29.

Son cómplices los que, no hallándose comprendidos en el artículo anterior, cooperan a la ejecución del hecho con actos anteriores o simultáneos.

Artículo 30.

1. En los delitos que se cometan utilizando medios o soportes de difusión mecánicos no responderán criminalmente ni los cómplices ni quienes los hubieren favorecido personal o realmente.

2. Los autores a los que se refiere el artículo 28 responderán de forma escalonada, excluyente y subsidiaria de acuerdo con el siguiente orden:

1.º Los que realmente hayan redactado el texto o producido el signo de que se trate, y quienes les hayan inducido a realizarlo.
2.º Los directores de la publicación o programa en que se difunda.
3.º Los directores de la empresa editora, emisora o difusora.
4.º Los directores de la empresa grabadora, reproductora o impresora.

3. Cuando por cualquier motivo distinto de la extinción de la responsabilidad penal, incluso la declaración de rebeldía o la residencia fuera de España, no pueda perseguirse a ninguna de las personas comprendidas en alguno de los números del apartado anterior, se dirigirá el procedimiento contra las mencionadas en el número inmediatamente posterior.

Artículo 31.

El que actúe como administrador de hecho o de derecho de una persona jurídica, o en nombre o representación legal o voluntaria de otro, responderá personalmente, aunque no concurran en él las condiciones, cualidades o relaciones que la correspondiente figura de delito requiera para poder ser sujeto activo del mismo, si tales circunstancias se dan en la entidad o persona en cuyo nombre o representación obre.

Artículo 31 bis.

1. En los supuestos previstos en este Código, las personas jurídicas serán penalmente responsables:

a) De los delitos cometidos en nombre o por cuenta de las mismas, y en su beneficio directo o indirecto, por sus representantes legales o por aquellos que actuando individualmente o como integrantes de un órgano de la persona jurídica, están autorizados para tomar decisiones en nombre de la persona jurídica u ostentan facultades de organización y control dentro de la misma.
b) De los delitos cometidos, en el ejercicio de actividades sociales y por cuenta y en beneficio directo o indirecto de las mismas, por quienes, estando sometidos a la autoridad de las personas físicas mencionadas en el párrafo anterior, han podido realizar los hechos por haberse incumplido gravemente por aquéllos los deberes de supervisión, vigilancia y control de su actividad atendidas las concretas circunstancias del caso.

2. Si el delito fuere cometido por las personas indicadas en la letra a) del apartado anterior, la persona jurídica quedará exenta de responsabilidad si se cumplen las siguientes condiciones:

1.ª el órgano de administración ha adoptado y ejecutado con eficacia, antes de la comisión del delito, modelos de organización y gestión que incluyen las medidas de vigilancia y control idóneas para prevenir delitos de la misma naturaleza o para reducir de forma significativa el riesgo de su comisión;
2.ª la supervisión del funcionamiento y del cumplimiento del modelo de prevención implantado ha sido confiada a un órgano de la persona jurídica con poderes autónomos de iniciativa y de control o que tenga encomendada legalmente la función de supervisar la eficacia de los controles internos de la persona jurídica;
3.ª los autores individuales han cometido el delito eludiendo fraudulentamente los modelos de organización y de prevención y
4.ª no se ha producido una omisión o un ejercicio insuficiente de sus funciones de supervisión, vigilancia y control por parte del órgano al que se refiere la condición 2.ª
En los casos en los que las anteriores circunstancias solamente puedan ser objeto de acreditación parcial, esta circunstancia será valorada a los efectos de atenuación de la pena.

3. En las personas jurídicas de pequeñas dimensiones, las funciones de supervisión a que se refiere la condición 2.ª del apartado 2 podrán ser asumidas directamente por el órgano de administración. A estos efectos, son personas jurídicas de pequeñas dimensiones aquéllas que, según la legislación aplicable, estén autorizadas a presentar cuenta de pérdidas y ganancias abreviada.

4. Si el delito fuera cometido por las personas indicadas en la letra b) del apartado 1, la persona jurídica quedará exenta de responsabilidad si, antes de la comisión del delito, ha adoptado y ejecutado eficazmente un modelo de organización y gestión que resulte adecuado para prevenir delitos de la naturaleza del que fue cometido o para reducir de forma significativa el riesgo de su comisión.

En este caso resultará igualmente aplicable la atenuación prevista en el párrafo segundo del apartado 2 de este artículo.

5. Los modelos de organización y gestión a que se refieren la condición 1.ª del apartado 2 y el apartado anterior deberán cumplir los siguientes requisitos:

1.º Identificarán las actividades en cuyo ámbito puedan ser cometidos los delitos que deben ser prevenidos.

2.º Establecerán los protocolos o procedimientos que concreten el proceso de formación de la voluntad de la persona jurídica, de adopción de decisiones y de ejecución de las mismas con relación a aquéllos.

3.º Dispondrán de modelos de gestión de los recursos financieros adecuados para impedir la comisión de los delitos que deben ser prevenidos.

4.º Impondrán la obligación de informar de posibles riesgos e incumplimientos al organismo encargado de vigilar el funcionamiento y observancia del modelo de prevención.

5.º Establecerán un sistema disciplinario que sancione adecuadamente el incumplimiento de las medidas que establezca el modelo.

6.º Realizarán una verificación periódica del modelo y de su eventual modificación cuando se pongan de manifiesto infracciones relevantes de sus disposiciones, o cuando se produzcan cambios en la organización, en la estructura de control o en la actividad desarrollada que los hagan necesarios.

Artículo 31 ter.

1. La responsabilidad penal de las personas jurídicas será exigible siempre que se constate la comisión de un delito que haya tenido que cometerse por quien ostente los cargos o funciones aludidas en el artículo anterior, aun cuando la concreta persona física responsable no haya sido individualizada o no haya sido posible dirigir el procedimiento contra ella. Cuando como consecuencia de los mismos hechos se impusiere a ambas la pena de multa, los jueces o tribunales modularán las respectivas cuantías, de modo que la suma resultante no sea desproporcionada en relación con la gravedad de aquéllos.

2. La concurrencia, en las personas que materialmente hayan realizado los hechos o en las que los hubiesen hecho posibles por no haber ejercido el debido control, de circunstancias que afecten a la culpabilidad del acusado o agraven su responsabilidad, o el hecho de que dichas personas hayan fallecido o se hubieren sustraído a la acción de la justicia, no excluirá ni modificará la responsabilidad penal de las personas jurídicas, sin perjuicio de lo que se dispone en el artículo siguiente.

Artículo 31 quater.

1. Sólo podrán considerarse circunstancias atenuantes de la responsabilidad penal de las personas jurídicas haber realizado, con posterioridad a la comisión del delito y a través de sus representantes legales, las siguientes actividades:

a) Haber procedido, antes de conocer que el procedimiento judicial se dirige contra ella, a confesar la infracción a las autoridades.

b) Haber colaborado en la investigación del hecho aportando pruebas, en cualquier momento del proceso, que fueran nuevas y decisivas para esclarecer las responsabilidades penales dimanantes de los hechos.

c) Haber procedido en cualquier momento del procedimiento y con anterioridad al juicio oral a reparar o disminuir el daño causado por el delito.

d) Haber establecido, antes del comienzo del juicio oral, medidas eficaces para prevenir y descubrir los delitos que en el futuro pudieran cometerse con los medios o bajo la cobertura de la persona jurídica.

Artículo 31 quinquies.

1. Las disposiciones relativas a la responsabilidad penal de las personas jurídicas no serán aplicables al Estado, a las Administraciones públicas territoriales e institucionales, a los Organismos Reguladores, las Agencias y Entidades públicas Empresariales, a las organizaciones internacionales de derecho público, ni a aquellas otras que ejerzan potestades públicas de soberanía o administrativas.

2. En el caso de las Sociedades mercantiles públicas que ejecuten políticas públicas o presten servicios de interés económico general, solamente les podrán ser impuestas las penas previstas en las letras a) y g) del apartado 7 del artículo 33. Esta limitación no será aplicable cuando el juez o tribunal aprecie que se trata de una forma jurídica creada por sus promotores, fundadores, administradores o representantes con el propósito de eludir una eventual responsabilidad penal.

[. . .]

TÍTULO V

De la responsabilidad civil derivada de los delitos y de las costas procesales

CAPÍTULO I

De la responsabilidad civil y su extensión

Artículo 109.

1. La ejecución de un hecho descrito por la ley como delito obliga a reparar, en los términos previstos en las leyes, los daños y perjuicios por él causados.

2. El perjudicado podrá optar, en todo caso, por exigir la responsabilidad civil ante la Jurisdicción Civil.

Artículo 110.

La responsabilidad establecida en el artículo anterior comprende:

1.º La restitución.
2.º La reparación del daño.
3.º La indemnización de perjuicios materiales y morales.

Artículo 111.

1. Deberá restituirse, siempre que sea posible, el mismo bien, con abono de los deterioros y menoscabos que el juez o tribunal determinen. La restitución tendrá lugar aunque el bien se halle en poder de tercero y éste lo haya adquirido legalmente y de buena fe, dejando a salvo su derecho de repetición contra quien corresponda y, en su caso, el de ser indemnizado por el responsable civil del delito.

2. Esta disposición no es aplicable cuando el tercero haya adquirido el bien en la forma y con los requisitos establecidos por las Leyes para hacerlo irreivindicable.

Artículo 112.

La reparación del daño podrá consistir en obligaciones de dar, de hacer o de no hacer que el Juez o Tribunal establecerá atendiendo a la naturaleza de aquél y a las condiciones personales y patrimoniales del culpable, determinando si han de ser cumplidas por él mismo o pueden ser ejecutadas a su costa.

Artículo 113.

La indemnización de perjuicios materiales y morales comprenderá no sólo los que se hubieren causado al agraviado, sino también los que se hubieren irrogado a sus familiares o a terceros.

Artículo 114.

Si la víctima hubiere contribuido con su conducta a la producción del daño o perjuicio sufrido, los Jueces o Tribunales podrán moderar el importe de su reparación o indemnización.

Artículo 115.

Los Jueces y Tribunales, al declarar la existencia de responsabilidad civil, establecerán razonadamente, en sus resoluciones las bases en que fundamenten la cuantía de los daños e indemnizaciones, pudiendo fijarla en la propia resolución o en el momento de su ejecución.

CAPÍTULO II

De las personas civilmente responsables

Artículo 116.

1. Toda persona criminalmente responsable de un delito lo es también civilmente si del hecho se derivaren daños o perjuicios. Si son dos o más los responsables de un delito los jueces o tribunales señalarán la cuota de que deba responder cada uno.

2. Los autores y los cómplices, cada uno dentro de su respectiva clase, serán responsables solidariamente entre sí por sus cuotas, y subsidiariamente por las correspondientes a los demás responsables.

La responsabilidad subsidiaria se hará efectiva: primero, en los bienes de los autores, y después, en los de los cómplices.

Tanto en los casos en que se haga efectiva la responsabilidad solidaria como la subsidiaria, quedará a salvo la repetición del que hubiere pagado contra los demás por las cuotas correspondientes a cada uno.

3. La responsabilidad penal de una persona jurídica llevará consigo su responsabilidad civil en los términos establecidos en el artículo 110 de este Código de forma solidaria con las personas físicas que fueren condenadas por los mismos hechos.

Artículo 117.

Los aseguradores que hubieren asumido el riesgo de las responsabilidades pecuniarias derivadas del uso o explotación de cualquier bien, empresa, industria o actividad, cuando, como consecuencia de un hecho previsto en este Código, se produzca el evento que determine el riesgo asegurado, serán responsables civiles directos hasta el límite de la indemnización legalmente establecida o convencionalmente pactada, sin perjuicio del derecho de repetición contra quien corresponda.

Artículo 118.

1. La exención de la responsabilidad criminal declarada en los números 1.º, 2.º, 3.º, 5.º y 6.º del artículo 20, no comprende la de la responsabilidad civil, que se hará efectiva conforme a las reglas siguientes:

1.ª En los casos de los números 1.º y 3.º, son también responsables por los hechos que ejecuten los declarados exentos de responsabilidad penal, quienes ejerzan su apoyo legal o de hecho, siempre que haya mediado culpa o negligencia por su parte y sin perjuicio de la responsabilidad civil directa que pudiera corresponder a los inimputables.

Los Jueces o Tribunales graduarán de forma equitativa la medida en que deba responder con sus bienes cada uno de dichos sujetos.

2.ª Son igualmente responsables el ebrio y el intoxicado en el supuesto del número 2.º

3.ª En el caso del número 5.º serán responsables civiles directos las personas en cuyo favor se haya precavido el mal, en proporción al perjuicio que se les haya evitado, si fuera estimable o, en otro caso, en la que el Juez o Tribunal establezca según su prudente arbitrio.

Cuando las cuotas de que deba responder el interesado no sean equitativamente asignables por el Juez o Tribunal, ni siquiera por aproximación, o cuando la responsabilidad se extienda a las Administraciones Públicas o a la mayor parte de una población y, en todo

caso, siempre que el daño se haya causado con asentimiento de la autoridad o de sus agentes, se acordará, en su caso, la indemnización en la forma que establezcan las leyes y reglamentos especiales.

4.ª En el caso del número 6.º, responderán principalmente los que hayan causado el miedo, y en defecto de ellos, los que hayan ejecutado el hecho.

2. En el caso del artículo 14, serán responsables civiles los autores del hecho.

Artículo 119.

En todos los supuestos del artículo anterior, el Juez o Tribunal que dicte sentencia absolutoria por estimar la concurrencia de alguna de las causas de exención citadas, procederá a fijar las responsabilidades civiles salvo que se haya hecho expresa reserva de las acciones para reclamarlas en la vía que corresponda.

Artículo 120.

Son también responsables civilmente, en defecto de los que lo sean criminalmente:

1.º Los curadores con facultades de representación plena que convivan con la persona a quien prestan apoyo, siempre que haya por su parte culpa o negligencia.

2.º Las personas naturales o jurídicas titulares de editoriales, periódicos, revistas, estaciones de radio o televisión o de cualquier otro medio de difusión escrita, hablada o visual, por los delitos cometidos utilizando los medios de los que sean titulares, dejando a salvo lo dispuesto en el artículo 212.

3.º Las personas naturales o jurídicas, en los casos de delitos cometidos en los establecimientos de los que sean titulares, cuando por parte de los que los dirijan o administren, o de sus dependientes o empleados, se hayan infringido los reglamentos de policía o las disposiciones de la autoridad que estén relacionados con el hecho punible cometido, de modo que éste no se hubiera producido sin dicha infracción.

4.º Las personas naturales o jurídicas dedicadas a cualquier género de industria o comercio, por los delitos que hayan cometido sus empleados o dependientes, representantes o gestores en el desempeño de sus obligaciones o servicios.

5.º Las personas naturales o jurídicas titulares de vehículos susceptibles de crear riesgos para terceros, por los delitos cometidos en la utilización de aquellos por sus dependientes o representantes o personas autorizadas.

Artículo 121.

El Estado, la Comunidad Autónoma, la provincia, la isla, el municipio y demás entes públicos, según los casos, responden subsidiariamente de los daños causados por los penalmente responsables de los delitos dolosos o culposos, cuando éstos sean autoridad, agentes y contratados de la misma o funcionarios públicos en el ejercicio de sus cargos o funciones siempre que la lesión sea consecuencia directa del funcionamiento de los servicios públicos que les estuvieren confiados, sin perjuicio de la responsabilidad patrimonial derivada del funcionamiento normal o anormal de dichos servicios exigible conforme a las normas de procedimiento administrativo, y sin que, en ningún caso, pueda darse una duplicidad indemnizatoria.

Si se exigiera en el proceso penal la responsabilidad civil de la autoridad, agentes y contratados de la misma o funcionarios públicos, la pretensión deberá dirigirse simultáneamente contra la Administración o ente público presuntamente responsable civil subsidiario.

Artículo 122.

El que por título lucrativo hubiere participado de los efectos de un delito, está obligado a la restitución de la cosa o al resarcimiento del daño hasta la cuantía de su participación.

[. . .]

CAPÍTULO II

De las amenazas

Artículo 169.

El que amenazare a otro con causarle a él, a su familia o a otras personas con las que esté íntimamente vinculado un mal que constituya delitos de homicidio, lesiones, aborto, contra la libertad, torturas y contra la integridad moral, la libertad sexual, la intimidad, el honor, el patrimonio y el orden socioeconómico, será castigado:

1.º Con la pena de prisión de uno a cinco años, si se hubiere hecho la amenaza exigiendo una cantidad o imponiendo cualquier otra condición, aunque no sea ilícita, y el culpable hubiere conseguido su propósito. De no conseguirlo, se impondrá la pena de prisión de seis meses a tres años.

Las penas señaladas en el párrafo anterior se impondrán en su mitad superior si las amenazas se hicieren por escrito, por teléfono o por cualquier medio de comunicación o de reproducción, o en nombre de entidades o grupos reales o supuestos.

2.º Con la pena de prisión de seis meses a dos años, cuando la amenaza no haya sido condicional.

Artículo 170.

1. Si las amenazas de un mal que constituyere delito fuesen dirigidas a atemorizar a los habitantes de una población, grupo étnico, cultural o religioso, o colectivo social o profesional, o a cualquier otro grupo de personas, y tuvieran la gravedad necesaria para conseguirlo, se impondrán respectivamente las penas superiores en grado a las previstas en el artículo anterior.

2. Serán castigados con la pena de prisión de seis meses a dos años, los que, con la misma finalidad y gravedad, reclamen públicamente la comisión de acciones violentas por parte de organizaciones o grupos terroristas.

Artículo 171.

1. Las amenazas de un mal que no constituya delito serán castigadas con pena de prisión de tres meses a un año o multa de seis a 24 meses, atendidas la gravedad y circunstancia del hecho, cuando la amenaza fuere condicional y la condición no consistiere en una conducta debida. Si el culpable hubiere conseguido su propósito se le impondrá la pena en su mitad superior.

2. Si alguien exigiere de otro una cantidad o recompensa bajo la amenaza de revelar o difundir hechos referentes a su vida privada o relaciones familiares que no sean públicamente conocidos y puedan afectar a su fama, crédito o interés, será castigado con la pena de prisión de dos a cuatro años, si ha conseguido la entrega de todo o parte de lo exigido, y con la de cuatro meses a dos años, si no lo consiguiere.

3. Si el hecho descrito en el apartado anterior consistiere en la amenaza de revelar o denunciar la comisión de algún delito el ministerio fiscal podrá, para facilitar el castigo de la amenaza, abstenerse de acusar por el delito cuya revelación se hubiere amenazado, salvo que éste estuviere castigado con pena de prisión superior a dos años. En este último caso, el juez o tribunal podrá rebajar la sanción en uno o dos grados.

4. El que de modo leve amenace a quien sea o haya sido su esposa, o mujer que esté o haya estado ligada a él por una análoga relación de afectividad aun sin convivencia, será castigado con la pena de prisión de seis meses a un año o de trabajos en beneficio de la comunidad de treinta y uno a ochenta días y, en todo caso, privación del derecho a la tenencia y porte de armas de un año y un día a tres años, así como, cuando el Juez o Tribunal lo estime adecuado al interés del menor o persona con discapacidad necesitada de especial protección, inhabilitación especial para el ejercicio de la patria potestad, tutela, curatela, guarda o acogimiento hasta cinco años.

Igual pena se impondrá al que de modo leve amenace a una persona especialmente vulnerable que conviva con el autor.

5. El que de modo leve amenace con armas u otros instrumentos peligrosos a alguna de las personas a las que se refiere el artículo 173.2, exceptuadas las contempladas en el apartado anterior de este artículo, será castigado con la pena de prisión de tres meses a un año o trabajos en beneficio de la comunidad de treinta y uno a ochenta días y, en todo caso, privación del derecho a la tenencia y porte de armas de uno a tres años, así como, cuando el Juez o Tribunal lo estime adecuado al interés del menor o persona con discapacidad necesitada de especial protección, inhabilitación especial para el ejercicio de la patria potestad, tutela, curatela, guarda o acogimiento por tiempo de seis meses a tres años.

Se impondrán las penas previstas en los apartados 4 y 5, en su mitad superior cuando el delito se perpetre en presencia de menores, o tenga lugar en el domicilio común o en el domicilio de la víctima, o se realice quebrantando una pena de las contempladas en el artículo 48 de este Código o una medida cautelar o de seguridad de la misma naturaleza.

6. No obstante lo previsto en los apartados 4 y 5, el Juez o Tribunal, razonándolo en sentencia, en atención a las circunstancias personales del autor y a las concurrentes en la realización del hecho, podrá imponer la pena inferior en grado.

7. Fuera de los casos anteriores, el que de modo leve amenace a otro será castigado con la pena de multa de uno a tres meses. Este hecho sólo será perseguible mediante denuncia de la persona agraviada o de su representante legal.

Cuando el ofendido fuere alguna de las personas a las que se refiere el apartado 2 del artículo 173, la pena será la de localización permanente de cinco a treinta días, siempre en domicilio diferente y alejado del de la víctima, o trabajos en beneficio de la comunidad de cinco a treinta días, o multa de uno a cuatro meses, ésta última únicamente en los supuestos en los que concurran las circunstancias expresadas en el apartado 2 del artículo 84. En estos casos no será exigible la denuncia a que se refiere el párrafo anterior.

CAPÍTULO III

De las coacciones

Artículo 172.

1. El que, sin estar legítimamente autorizado, impidiere a otro con violencia hacer lo que la ley no prohíbe, o le compeliere a efectuar lo que no quiere, sea justo o injusto, será castigado con la pena de prisión de seis meses a tres años o con multa de 12 a 24 meses, según la gravedad de la coacción o de los medios empleados.

Cuando la coacción ejercida tuviera como objeto impedir el ejercicio de un derecho fundamental se le impondrán las penas en su mitad superior, salvo que el hecho tuviera señalada mayor pena en otro precepto de este Código.

También se impondrán las penas en su mitad superior cuando la coacción ejercida tuviera por objeto impedir el legítimo disfrute de la vivienda.

2. El que de modo leve coaccione a quien sea o haya sido su esposa, o mujer que esté o haya estado ligada a él por una análoga relación de afectividad, aun sin convivencia, será castigado con la pena de prisión de seis meses a un año o de trabajos en beneficio de la comunidad de treinta y uno a ochenta días y, en todo caso, privación del derecho a la tenencia y porte de armas de un año y un día a tres años, así como, cuando el Juez o Tribunal lo estime adecuado al interés del menor o persona con discapacidad necesitada de especial protección, inhabilitación especial para el ejercicio de la patria potestad, tutela, curatela, guarda o acogimiento hasta cinco años.

Igual pena se impondrá al que de modo leve coaccione a una persona especialmente vulnerable que conviva con el autor.

Se impondrá la pena en su mitad superior cuando el delito se perpetre en presencia de menores, o tenga lugar en el domicilio común o en el domicilio de la víctima, o se realice quebrantando una pena de las contempladas en el artículo 48 de este Código o una medida cautelar o de seguridad de la misma naturaleza.

No obstante lo previsto en los párrafos anteriores, el Juez o Tribunal, razonándolo en sentencia, en atención a las circunstancias personales del autor y a las concurrentes en la realización del hecho, podrá imponer la pena inferior en grado.

3. Fuera de los casos anteriores, el que cause a otro una coacción de carácter leve, será castigado con la pena de multa de uno a tres meses. Este hecho sólo será perseguible mediante denuncia de la persona agraviada o de su representante legal.

Cuando el ofendido fuere alguna de las personas a las que se refiere el apartado 2 del artículo 173, la pena será la de localización permanente de cinco a treinta días, siempre en domicilio diferente y alejado del de la víctima, o trabajos en beneficio de la comunidad de cinco a treinta días, o multa de uno a cuatro meses, ésta última únicamente en los supuestos en los que concurran las circunstancias expresadas en el apartado 2 del artículo 84. En estos casos no será exigible la denuncia a que se refiere el párrafo anterior.

Artículo 172 bis.

1. El que con intimidación grave o violencia compeliere a otra persona a contraer matrimonio será castigado con una pena de prisión de seis meses a tres años y seis meses o con multa de doce a veinticuatro meses, según la gravedad de la coacción o de los medios empleados.

2. La misma pena se impondrá a quien, con la finalidad de cometer los hechos a que se refiere el apartado anterior, utilice violencia, intimidación grave o engaño para forzar a otro a abandonar el territorio español o a no regresar al mismo.

3. Las penas se impondrán en su mitad superior cuando la víctima fuera menor de edad.

4. En las sentencias condenatorias por delito de matrimonio forzado, además del pronunciamiento correspondiente a la responsabilidad civil, se harán, en su caso, los que procedan en orden a la declaración de nulidad o disolución del matrimonio así contraído y a la filiación y fijación de alimentos.

Artículo 172 ter.

1. Será castigado con la pena de prisión de tres meses a dos años o multa de seis a veinticuatro meses el que acose a una persona llevando a cabo de forma insistente y reiterada, y sin estar legítimamente autorizado, alguna de las conductas siguientes y, de esta forma, altere el normal desarrollo de su vida cotidiana:

1.ª La vigile, la persiga o busque su cercanía física.

2.ª Establezca o intente establecer contacto con ella a través de cualquier medio de comunicación, o por medio de terceras personas.

3.ª Mediante el uso indebido de sus datos personales, adquiera productos o mercancías, o contrate servicios, o haga que terceras personas se pongan en contacto con ella.

4.ª Atente contra su libertad o contra su patrimonio, o contra la libertad o patrimonio de otra persona próxima a ella. Cuando la víctima se halle en una situación de especial vulnerabilidad por razón de su edad, enfermedad, discapacidad o por cualquier otra circunstancia, se impondrá la pena de prisión de seis meses a dos años.

2. Cuando el ofendido fuere alguna de las personas a las que se refiere el apartado 2 del artículo 173, se impondrá una pena de prisión de uno a dos años, o trabajos en beneficio de la comunidad de sesenta a ciento veinte días. En este caso no será necesaria la denuncia a que se refiere el apartado 4 de este artículo.

3. Las penas previstas en este artículo se impondrán sin perjuicio de las que pudieran corresponder a los delitos en que se hubieran concretado los actos de acoso.

4. Los hechos descritos en este artículo sólo serán perseguibles mediante denuncia de la persona agraviada o de su representante legal.

5. El que, sin consentimiento de su titular, utilice la imagen de una persona para realizar anuncios o abrir perfiles falsos en redes sociales, páginas de contacto o cualquier medio de difusión pública, ocasionándole a la misma situación de acoso, hostigamiento o humillación, será castigado con pena de prisión de tres meses a un año o multa de seis a doce meses. Si la víctima del delito es un menor o una persona con discapacidad, se aplicará la mitad superior de la condena.

Artículo 172 quater.

1. El que para obstaculizar el ejercicio del derecho a la interrupción voluntaria del embarazo acosare a una mujer mediante actos molestos, ofensivos, intimidatorios o

coactivos que menoscaben su libertad, será castigado con la pena de prisión de tres meses a un año o de trabajos en beneficio de la comunidad de treinta y uno a ochenta días.

2. Las mismas penas se impondrán a quien, en la forma descrita en el apartado anterior, acosare a los trabajadores del ámbito sanitario en su ejercicio profesional o función pública y al personal facultativo o directivo de los centros habilitados para interrumpir el embarazo con el objetivo de obstaculizar el ejercicio de su profesión o cargo.

3. Atendidas la gravedad, las circunstancias personales del autor y las concurrentes en la realización del hecho, el tribunal podrá imponer, además, la prohibición de acudir a determinados lugares por tiempo de seis meses a tres años.

4. Las penas previstas en este artículo se impondrán sin perjuicio de las que pudieran corresponder a los delitos en que se hubieran concretado los actos de acoso.

5. En la persecución de los hechos descritos en este artículo no será necesaria la denuncia de la persona agraviada ni de su representación legal.

[. . .]

CAPÍTULO IV

De los delitos de exhibicionismo y provocación sexual

Artículo 185.

El que ejecutare o hiciere ejecutar a otra persona actos de exhibición obscena ante menores de edad o personas con discapacidad necesitadas de especial protección, será castigado con la pena de prisión de seis meses a un año o multa de 12 a 24 meses.

Artículo 186.

El que, por cualquier medio directo, vendiere, difundiere o exhibiere material pornográfico entre menores de edad o personas con discapacidad necesitadas de especial protección, será castigado con la pena de prisión de seis meses a un año o multa de 12 a 24 meses.

CAPÍTULO V

De los delitos relativos a la prostitución y a la explotación sexual y corrupción de menores.

Artículo 187.

1. El que, empleando violencia, intimidación o engaño, o abusando de una situación de superioridad o de necesidad o vulnerabilidad de la víctima, determine a una persona mayor de edad a ejercer o a mantenerse en la prostitución, será castigado con las penas de prisión de dos a cinco años y multa de doce a veinticuatro meses.

Se impondrá la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses a quien se lucre explotando la prostitución de otra persona, aun con el consentimiento de la misma. En todo caso, se entenderá que hay explotación cuando concurra alguna de las siguientes circunstancias:

a) Que la víctima se encuentre en una situación de vulnerabilidad personal o económica.

b) Que se le impongan para su ejercicio condiciones gravosas, desproporcionadas o abusivas.

2. Se impondrán las penas previstas en los apartados anteriores en su mitad superior, en sus respectivos casos, cuando concurra alguna de las siguientes circunstancias:

a) Cuando el culpable se hubiera prevalido de su condición de autoridad, agente de ésta o funcionario público. En este caso se aplicará, además, la pena de inhabilitación absoluta de seis a doce años.

b) Cuando el culpable perteneciere a una organización o grupo criminal que se dedicare a la realización de tales actividades.

c) Cuando el culpable hubiere puesto en peligro, de forma dolosa o por imprudencia grave, la vida o salud de la víctima.

3. Las penas señaladas se impondrán en sus respectivos casos sin perjuicio de las que correspondan por las agresiones o abusos sexuales cometidos sobre la persona prostituida.

Artículo 188.

1. El que induzca, promueva, favorezca o facilite la prostitución de un menor de edad o una persona con discapacidad necesitada de especial protección, o se lucre con ello, o explote de algún otro modo a un menor o a una persona con discapacidad para estos fines, será castigado con las penas de prisión de dos a cinco años y multa de doce a veinticuatro meses.

Si la víctima fuera menor de dieciséis años, se impondrá la pena de prisión de cuatro a ocho años y multa de doce a veinticuatro meses.

2. Si los hechos descritos en el apartado anterior se cometieran con violencia o intimidación, además de las penas de multa previstas, se impondrá la pena de prisión de cinco a diez años si la víctima es menor de dieciséis años, y la pena de prisión de cuatro a seis años en los demás casos.

3. Se impondrán las penas superiores en grado a las previstas en los apartados anteriores, en sus respectivos casos, cuando concurra alguna de las siguientes circunstancias:

a) Cuando la víctima se halle en una situación de especial vulnerabilidad por razón de su edad, enfermedad, discapacidad o por cualquier otra circunstancia.

b) Cuando, para la ejecución del delito, el responsable se hubiera prevalido de una situación de convivencia o de una relación de superioridad o parentesco, por ser ascendiente, o hermano, por naturaleza o adopción, o afines, con la víctima.

c) Cuando, para la ejecución del delito, el responsable se hubiera prevalido de su condición de autoridad, agente de ésta o funcionario público. En este caso se impondrá, además, una pena de inhabilitación absoluta de seis a doce años.

d) Cuando el culpable hubiere puesto en peligro, de forma dolosa o por imprudencia grave, la vida o salud de la víctima.

e) Cuando los hechos se hubieren cometido por la actuación conjunta de dos o más personas.

f) Cuando el culpable perteneciere a una organización o asociación, incluso de carácter transitorio, que se dedicare a la realización de tales actividades.

4. El que solicite, acepte u obtenga, a cambio de una remuneración o promesa, una relación sexual con una persona menor de edad o una persona con discapacidad necesitada de especial protección, será castigado con una pena de uno a cuatro años de prisión. Si el menor no hubiera cumplido dieciséis años de edad, se impondrá una pena de dos a seis años de prisión.

5. Las penas señaladas se impondrán en sus respectivos casos sin perjuicio de las que correspondan por las infracciones contra la libertad o indemnidad sexual cometidas sobre los menores y personas con discapacidad necesitadas de especial protección.

Artículo 189.

1. Será castigado con la pena de prisión de uno a cinco años:

a) El que captare o utilizare a menores de edad o a personas con discapacidad necesitadas de especial protección con fines o en espectáculos exhibicionistas o pornográficos, tanto públicos como privados, o para elaborar cualquier clase de material pornográfico, cualquiera que sea su soporte, o financiare cualquiera de estas actividades o se lucrare con ellas.

b) El que produjere, vendiere, distribuyere, exhibiere, ofreciere o facilitare la producción, venta, difusión o exhibición por cualquier medio de pornografía infantil o en cuya elaboración hayan sido utilizadas personas con discapacidad necesitadas de especial protección, o lo poseyere para estos fines, aunque el material tuviere su origen en el extranjero o fuere desconocido.

A los efectos de este Título se considera pornografía infantil o en cuya elaboración hayan sido utilizadas personas con discapacidad necesitadas de especial protección:

a) Todo material que represente de manera visual a un menor o una persona con discapacidad necesitada de especial protección participando en una conducta sexualmente explícita, real o simulada.

b) Toda representación de los órganos sexuales de un menor o persona con discapacidad necesitada de especial protección con fines principalmente sexuales.

c) Todo material que represente de forma visual a una persona que parezca ser un menor participando en una conducta sexualmente explícita, real o simulada, o cualquier representación de los órganos sexuales de una persona que parezca ser un menor, con fines principalmente sexuales, salvo que la persona que parezca ser un menor resulte tener en realidad dieciocho años o más en el momento de obtenerse las imágenes.

d) Imágenes realistas de un menor participando en una conducta sexualmente explícita o imágenes realistas de los órganos sexuales de un menor, con fines principalmente sexuales.

2. Serán castigados con la pena de prisión de cinco a nueve años los que realicen los actos previstos en el apartado 1 de este artículo cuando concurra alguna de las circunstancias siguientes:

a) Cuando se utilice a menores de dieciséis años.

b) Cuando los hechos revistan un carácter particularmente degradante o vejatorio, se emplee violencia física o sexual para la obtención del material pornográfico o se representen escenas de violencia física o sexual.

c) Cuando se utilice a personas menores de edad que se hallen en una situación de especial vulnerabilidad por razón de enfermedad, discapacidad o por cualquier otra circunstancia.

d) Cuando el culpable hubiere puesto en peligro, de forma dolosa o por imprudencia grave, la vida o salud de la víctima.

e) Cuando el material pornográfico fuera de notoria importancia.

f) Cuando el culpable perteneciere a una organización o asociación, incluso de carácter transitorio, que se dedicare a la realización de tales actividades.

g) Cuando el responsable sea ascendiente, tutor, curador, guardador, maestro o cualquier otra persona encargada, de hecho, aunque fuera provisionalmente, o de derecho, de la persona menor de edad o persona con discapacidad necesitada de especial protección, o se trate de cualquier persona que conviva con él o de otra persona que haya actuado abusando de su posición reconocida de confianza o autoridad.

h) Cuando concurra la agravante de reincidencia.

3. Si los hechos a que se refiere la letra a) del párrafo primero del apartado 1 se hubieran cometido con violencia o intimidación se impondrá la pena superior en grado a las previstas en los apartados anteriores.

4. El que asistiere a sabiendas a espectáculos exhibicionistas o pornográficos en los que participen menores de edad o personas con discapacidad necesitadas de especial protección, será castigado con la pena de seis meses a dos años de prisión.

5. El que para su propio uso adquiera o posea pornografía infantil o en cuya elaboración se hubieran utilizado personas con discapacidad necesitadas de especial protección, será castigado con la pena de tres meses a un año de prisión o con multa de seis meses a dos años.

La misma pena se impondrá a quien acceda a sabiendas a pornografía infantil o en cuya elaboración se hubieran utilizado personas con discapacidad necesitadas de especial protección, por medio de las tecnologías de la información y la comunicación.

6. El que tuviere bajo su potestad, tutela, guarda o acogimiento a un menor de edad o una persona con discapacidad necesitada de especial protección y que, con conocimiento de su estado de prostitución o corrupción, no haga lo posible para impedir su continuación en tal estado, o no acuda a la autoridad competente para el mismo fin si carece de medios para la custodia del menor o persona con discapacidad necesitada de especial protección, será castigado con la pena de prisión de tres a seis meses o multa de seis a doce meses.

7. El Ministerio Fiscal promoverá las acciones pertinentes con objeto de privar de la patria potestad, tutela, guarda o acogimiento familiar, en su caso, a la persona que incurra en alguna de las conductas descritas en el apartado anterior.

8. Los jueces y tribunales ordenarán la adopción de las medidas necesarias para la retirada de las páginas web o aplicaciones de internet que contengan o difundan pornografía infantil o en cuya elaboración se hubieran utilizado personas con discapacidad necesitadas de especial protección o, en su caso, para bloquear el acceso a las mismas a los usuarios de Internet que se encuentren en territorio español.

Estas medidas podrán ser acordadas con carácter cautelar a petición del Ministerio Fiscal.

Artículo 189 bis.

La distribución o difusión pública a través de Internet, del teléfono o de cualquier otra tecnología de la información o de la comunicación de contenidos específicamente destinados a promover, fomentar o incitar a la comisión de los delitos previstos en este capítulo y en los capítulos II y IV del presente título será castigada con la pena de multa de seis a doce meses o pena de prisión de uno a tres años.

Las autoridades judiciales ordenarán la adopción de las medidas necesarias para la retirada de los contenidos a los que se refiere el párrafo anterior, para la interrupción de los servicios que ofrezcan predominantemente dichos contenidos o para el bloqueo de unos y otros cuando radiquen en el extranjero.

Artículo 189 ter.

Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en este Capítulo, se le impondrán las siguientes penas:

a) Multa del triple al quíntuple del beneficio obtenido, si el delito cometido por la persona física tiene prevista una pena de prisión de más de cinco años.

b) Multa del doble al cuádruple del beneficio obtenido, si el delito cometido por la persona física tiene prevista una pena de prisión de más de dos años no incluida en el anterior inciso.

c) Multa del doble al triple del beneficio obtenido, en el resto de los casos.

d) Disolución de la persona jurídica, conforme a lo dispuesto en el artículo 33.7 b) de este Código, pudiendo decretarse, atendidas las reglas recogidas en el artículo 66 bis, las demás penas previstas en el mismo que sean compatibles con la disolución.

CAPÍTULO VI

Disposiciones comunes a los capítulos anteriores

Artículo 190.

La condena de un Juez o Tribunal extranjero, impuesta por delitos comprendidos en este Título, será equiparada a las sentencias de los Jueces o Tribunales españoles a los efectos de la aplicación de la circunstancia agravante de reincidencia.

[. . .]

TÍTULO X

Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio

CAPÍTULO I

Del descubrimiento y revelación de secretos

Artículo 197.

1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

3. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.

Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.

4. Los hechos descritos en los apartados 1 y 2 de este artículo serán castigados con una pena de prisión de tres a cinco años cuando:

a) Se cometan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros; o

b) se lleven a cabo mediante la utilización no autorizada de datos personales de la víctima.

Si los datos reservados se hubieran difundido, cedido o revelado a terceros, se impondrán las penas en su mitad superior.

5. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o una persona con discapacidad necesitada de especial protección, se impondrán las penas previstas en su mitad superior.

6. Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado anterior, la pena a imponer será la de prisión de cuatro a siete años.

7. Será castigado con una pena de prisión de tres meses a un año o multa de seis a doce meses el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona.

Se impondrá la pena de multa de uno a tres meses a quien habiendo recibido las imágenes o grabaciones audiovisuales a las que se refiere el párrafo anterior las difunda, revele o ceda a terceros sin el consentimiento de la persona afectada.

En los supuestos de los párrafos anteriores, la pena se impondrá en su mitad superior cuando los hechos hubieran sido cometidos por el cónyuge o por persona que esté o haya estado unida a él por análoga relación de afectividad, aun sin convivencia, la víctima fuera menor de edad o una persona con discapacidad necesitada de especial protección, o los hechos se hubieran cometido con una finalidad lucrativa.

Artículo 197 bis.

1. El que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.

2. El que mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos, será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses.

Artículo 197 ter.

Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los apartados 1 y 2 del artículo 197 o el artículo 197 bis:

a) un programa informático, concebido o adaptado principalmente para cometer dichos delitos; o

b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información.

Artículo 197 quater.

Si los hechos descritos en este Capítulo se hubieran cometido en el seno de una organización o grupo criminal, se aplicarán respectivamente las penas superiores en grado.

Artículo 197 quinquies.

Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en los artículos 197, 197 bis y 197 ter, se le impondrá la pena de multa de seis meses a dos años. Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33.

Artículo 198.

La autoridad o funcionario público que, fuera de los casos permitidos por la Ley, sin mediar causa legal por delito, y prevaliéndose de su cargo, realizare cualquiera de las conductas descritas en el artículo anterior, será castigado con las penas respectivamente previstas en el mismo, en su mitad superior y, además, con la de inhabilitación absoluta por tiempo de seis a doce años.

Artículo 199.

1. El que revelare secretos ajenos, de los que tenga conocimiento por razón de su oficio o sus relaciones laborales, será castigado con la pena de prisión de uno a tres años y multa de seis a doce meses.

2. El profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona, será castigado con la pena de prisión de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años.

Artículo 200.

Lo dispuesto en este capítulo será aplicable al que descubriere, revelare o cediere datos reservados de personas jurídicas, sin el consentimiento de sus representantes, salvo lo dispuesto en otros preceptos de este Código.

Artículo 201.

1. Para proceder por los delitos previstos en este Capítulo será necesaria denuncia de la persona agraviada o de su representante legal.

2. No será precisa la denuncia exigida en el apartado anterior para proceder por los hechos descritos en el artículo 198 de este Código, ni cuando la comisión del delito afecte a los intereses generales, a una pluralidad de personas o si la víctima es una persona menor de edad o una persona con discapacidad necesitada de especial protección.

3. El perdón del ofendido o de su representante legal, en su caso, extingue la acción penal sin perjuicio de lo dispuesto en el artículo 130.1.5.º, párrafo segundo.

[. . .]

TÍTULO XI

Delitos contra el honor

CAPÍTULO I

De la calumnia

Artículo 205.

Es calumnia la imputación de un delito hecha con conocimiento de su falsedad o temerario desprecio hacia la verdad.

Artículo 206.

Las calumnias serán castigadas con las penas de prisión de seis meses a dos años o multa de doce a 24 meses, si se propagaran con publicidad y, en otro caso, con multa de seis a 12 meses.

Artículo 207.

El acusado por delito de calumnia quedará exento de toda pena probando el hecho criminal que hubiere imputado.

CAPÍTULO II

De la injuria

Artículo 208.

Es injuria la acción o expresión que lesionan la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación.

Solamente serán constitutivas de delito las injurias que, por su naturaleza, efectos y circunstancias, sean tenidas en el concepto público por graves, sin perjuicio de lo dispuesto en el apartado 4 del artículo 173.

Las injurias que consistan en la imputación de hechos no se considerarán graves, salvo cuando se hayan llevado a cabo con conocimiento de su falsedad o temerario desprecio hacia la verdad.

Artículo 209.

Las injurias graves hechas con publicidad se castigarán con la pena de multa de seis a catorce meses y, en otro caso, con la de tres a siete meses.

Artículo 210.

El acusado de injuria quedará exento de responsabilidad probando la verdad de las imputaciones cuando estas se dirijan contra funcionarios públicos sobre hechos

concernientes al ejercicio de sus cargos o referidos a la comisión de infracciones administrativas.

CAPÍTULO III

Disposiciones generales

Artículo 211.

La calumnia y la injuria se reputarán hechas con publicidad cuando se propaguen por medio de la imprenta, la radiodifusión o por cualquier otro medio de eficacia semejante.

Artículo 212.

En los casos a los que se refiere el artículo anterior, será responsable civil solidaria la persona física o jurídica propietaria del medio informativo a través del cual se haya propagado la calumnia o injuria.

Artículo 213.

Si la calumnia o injuria fueren cometidas mediante precio, recompensa o promesa, los Tribunales impondrán, además de las penas señaladas para los delitos de que se trate, la de inhabilitación especial prevista en los artículos 42 ó 45 del presente Código, por tiempo de seis meses a dos años.

Artículo 214.

Si el acusado de calumnia o injuria reconociere ante la autoridad judicial la falsedad o falta de certeza de las imputaciones y se retractare de ellas, el Juez o Tribunal impondrá la pena inmediatamente inferior en grado y podrá dejar de imponer la pena de inhabilitación que establece el artículo anterior.

El Juez o Tribunal ante quien se produjera el reconocimiento ordenará que se entregue testimonio de retractación al ofendido y, si éste lo solicita, ordenará su publicación en el mismo medio en que se vertió la calumnia o injuria, en espacio idéntico o similar a aquél en que se produjo su difusión y dentro del plazo que señale el Juez o Tribunal sentenciador.

Artículo 215.

1. Nadie será penado por calumnia o injuria sino en virtud de querella de la persona ofendida por el delito o de su representante legal. Se procederá de oficio cuando la ofensa se dirija contra funcionario público, autoridad o agente de la misma sobre hechos concernientes al ejercicio de sus cargos.

2. Nadie podrá deducir acción de calumnia o injuria vertidas en juicio sin previa licencia del Juez o Tribunal que de él conociere o hubiere conocido.

3. El perdón de la persona ofendida extingue la acción penal, sin perjuicio de lo dispuesto en el artículo 130.1.5.º, párrafo segundo de este Código.

Artículo 216.

En los delitos de calumnia o injuria se considera que la reparación del daño comprende también la publicación o divulgación de la sentencia condenatoria, a costa del condenado por tales delitos, en el tiempo y forma que el Juez o Tribunal consideren más adecuado a tal fin, oídas las dos partes.

[. . .]

Sección 1.ª De las estafas

Artículo 248.

Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.

Los reos de estafa serán castigados con la pena de prisión de seis meses a tres años. Para la fijación de la pena se tendrá en cuenta el importe de lo defraudado, el quebranto económico causado al perjudicado, las relaciones entre este y el defraudador, los medios empleados por este y cuantas otras circunstancias sirvan para valorar la gravedad de la infracción.

Si la cuantía de lo defraudado no excediere de 400 euros, se impondrá la pena de multa de uno a tres meses.

Artículo 249.

1. También se consideran reos de estafa y serán castigados con la pena de prisión de seis meses a tres años:

a) Los que, con ánimo de lucro, obstaculizando o interfiriendo indebidamente en el funcionamiento de un sistema de información o introduciendo, alterando, borrando, transmitiendo o suprimiendo indebidamente datos informáticos o valiéndose de cualquier otra manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.

b) Los que, utilizando de forma fraudulenta tarjetas de crédito o débito, cheques de viaje o cualquier otro instrumento de pago material o inmaterial distinto del efectivo o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero.

2. Con la misma pena prevista en el apartado anterior serán castigados:

a) Los que fabricaren, importaren, obtuvieren, poseyeren, transportaren, comerciaren o de otro modo facilitaren a terceros dispositivos, instrumentos o datos o programas informáticos, o cualquier otro medio diseñado o adaptado específicamente para la comisión de las estafas previstas en este artículo.

b) Los que, para su utilización fraudulenta, sustraigan, se apropiaren o adquieran de forma ilícita tarjetas de crédito o débito, cheques de viaje o cualquier otro instrumento de pago material o inmaterial distinto del efectivo.

3. Se impondrá la pena en su mitad inferior a los que, para su utilización fraudulenta y sabiendo que fueron obtenidos ilícitamente, posean, adquieran, transfieran, distribuyan o pongan a disposición de terceros tarjetas de crédito o débito, cheques de viaje o cualesquiera otros instrumentos de pago materiales o inmateriales distintos del efectivo.

Artículo 250.

1. El delito de estafa será castigado con las penas de prisión de uno a seis años y multa de seis a doce meses, cuando:

1.º Recaiga sobre cosas de primera necesidad, viviendas u otros bienes de reconocida utilidad social.

2.º Se perpetre abusando de firma de otro, o sustrayendo, ocultando o inutilizando, en todo o en parte, algún proceso, expediente, protocolo o documento público u oficial de cualquier clase.

3.º Recaiga sobre bienes que integren el patrimonio artístico, histórico, cultural o científico.

4.º Revista especial gravedad, atendiendo a la entidad del perjuicio y a la situación económica en que deje a la víctima o a su familia.

5.º El valor de la defraudación supere los 50.000 euros, o afecte a un elevado número de personas.

6.º Se cometa con abuso de las relaciones personales existentes entre víctima y defraudador, o aproveche éste su credibilidad empresarial o profesional.

7.º Se cometa estafa procesal. Incurren en la misma los que, en un procedimiento judicial de cualquier clase, manipularen las pruebas en que pretendieran fundar sus alegaciones o emplearen otro fraude procesal análogo, provocando error en el juez o tribunal y llevándole a dictar una resolución que perjudique los intereses económicos de la otra parte o de un tercero.

8.º Al delinquir el culpable hubiera sido condenado ejecutoriamente al menos por tres delitos comprendidos en este Capítulo. No se tendrán en cuenta antecedentes cancelados o que debieran serlo.

2. Si concurrieran las circunstancias incluidas en los numerales 4.º, 5.º, 6.º o 7.º con la del numeral 1.º del apartado anterior, se impondrán las penas de prisión de cuatro a ocho años y multa de doce a veinticuatro meses. La misma pena se impondrá cuando el valor de la defraudación supere los 250.000 euros.

Artículo 251.

Será castigado con la pena de prisión de uno a cuatro años:

1.º Quien, atribuyéndose falsamente sobre una cosa mueble o inmueble facultad de disposición de la que carece, bien por no haberla tenido nunca, bien por haberla ya ejercitado, la enajenare, gravare o arrendare a otro, en perjuicio de éste o de tercero.

2.º El que dispusiere de una cosa mueble o inmueble ocultando la existencia de cualquier carga sobre la misma, o el que, habiéndola enajenado como libre, la gravare o enajenare nuevamente antes de la definitiva transmisión al adquirente, en perjuicio de éste, o de un tercero.

3.º El que otorgare en perjuicio de otro un contrato simulado.

Artículo 251 bis.

Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en esta Sección, se le impondrán las siguientes penas:

a) Multa del triple al quíntuple de la cantidad defraudada, si el delito cometido por la persona física tiene prevista una pena de prisión de más de cinco años.

b) Multa del doble al cuádruple de la cantidad defraudada, en el resto de los casos.

Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33.

[. . .]

Artículo 263.

1. El que causare daños en propiedad ajena no comprendidos en otros títulos de este Código, será castigado con multa de seis a veinticuatro meses, atendidas la condición económica de la víctima y la cuantía del daño.

Si la cuantía del daño causado no excediere de 400 euros, se impondrá una pena de multa de uno a tres meses.

2. Será castigado con la pena de prisión de uno a tres años y multa de doce a veinticuatro meses el que causare daños expresados en el apartado anterior, si concurriere alguno de los supuestos siguientes:

1.º Que se realicen para impedir el libre ejercicio de la autoridad o como consecuencia de acciones ejecutadas en el ejercicio de sus funciones, bien se cometiere el delito contra funcionarios públicos, bien contra particulares que, como testigos o de cualquier otra manera, hayan contribuido o puedan contribuir a la ejecución o aplicación de las Leyes o disposiciones generales.

2.º Que se cause por cualquier medio, infección o contagio de ganado.

3.º Que se empleen sustancias venenosas o corrosivas.

4.º Que afecten a bienes de dominio o uso público o comunal.

5.º Que arruinen al perjudicado o se le coloque en grave situación económica.

6.º Se hayan ocasionado daños de especial gravedad o afectado a los intereses generales.

Artículo 264.

1. El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a tres años.

2. Se impondrá una pena de prisión de dos a cinco años y multa del tanto al décuplo del perjuicio ocasionado, cuando en las conductas descritas concurra alguna de las siguientes circunstancias:

1.ª Se hubiese cometido en el marco de una organización criminal.

2.ª Haya ocasionado daños de especial gravedad o afectado a un número elevado de sistemas informáticos.

3.ª El hecho hubiera perjudicado gravemente el funcionamiento de servicios públicos esenciales o la provisión de bienes de primera necesidad.

4.ª Los hechos hayan afectado al sistema informático de una infraestructura crítica o se hubiera creado una situación de peligro grave para la seguridad del Estado, de la Unión Europea o de un Estado Miembro de la Unión Europea. A estos efectos se considerará infraestructura crítica un elemento, sistema o parte de este que sea esencial para el mantenimiento de funciones vitales de la sociedad, la salud, la seguridad, la protección y el bienestar económico y social de la población cuya perturbación o destrucción tendría un impacto significativo al no poder mantener sus funciones.

5.ª El delito se haya cometido utilizando alguno de los medios a que se refiere el artículo 264 ter.

Si los hechos hubieran resultado de extrema gravedad, podrá imponerse la pena superior en grado.

3. Las penas previstas en los apartados anteriores se impondrán, en sus respectivos casos, en su mitad superior, cuando los hechos se hubieran cometido mediante la utilización ilícita de datos personales de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero.

Artículo 264 bis.

1. Será castigado con la pena de prisión de seis meses a tres años el que, sin estar autorizado y de manera grave, obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno:

a) realizando alguna de las conductas a que se refiere el artículo anterior;

b) introduciendo o transmitiendo datos; o

c) destruyendo, dañando, inutilizando, eliminando o sustituyendo un sistema informático, telemático o de almacenamiento de información electrónica.

Si los hechos hubieran perjudicado de forma relevante la actividad normal de una empresa, negocio o de una Administración pública, se impondrá la pena en su mitad superior, pudiéndose alcanzar la pena superior en grado.

2. Se impondrá una pena de prisión de tres a ocho años y multa del triplo al décuplo del perjuicio ocasionado, cuando en los hechos a que se refiere el apartado anterior hubiera concurrido alguna de las circunstancias del apartado 2 del artículo anterior.

3. Las penas previstas en los apartados anteriores se impondrán, en sus respectivos casos, en su mitad superior, cuando los hechos se hubieran cometido mediante la utilización ilícita de datos personales de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero.

Artículo 264 ter.

Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso,

importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los dos artículos anteriores:

a) un programa informático, concebido o adaptado principalmente para cometer alguno de los delitos a que se refieren los dos artículos anteriores; o

b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información.

Artículo 264 quater.

Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en los tres artículos anteriores, se le impondrán las siguientes penas:

a) Multa de dos a cinco años o del quíntuplo a doce veces el valor del perjuicio causado, si resulta una cantidad superior, cuando se trate de delitos castigados con una pena de prisión de más de tres años.

b) Multa de uno a tres años o del triple a ocho veces el valor del perjuicio causado, si resulta una cantidad superior, en el resto de los casos.

Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33.

Artículo 265.

El que destruyere, dañare de modo grave, o inutilizare para el servicio, aun de forma temporal, obras, establecimientos o instalaciones militares, buques de guerra, aeronaves militares, medios de transporte o transmisión militar, material de guerra, aprovisionamiento u otros medios o recursos afectados al servicio de las Fuerzas Armadas o de las Fuerzas y Cuerpos de Seguridad, será castigado con la pena de prisión de dos a cuatro años si el daño causado excediere de mil euros.

Artículo 266.

1. Será castigado con la pena de prisión de uno a tres años el que cometiere los daños previstos en el apartado 1 del artículo 263 mediante incendio, o provocando explosiones, o utilizando cualquier otro medio de similar potencia destructiva o que genere un riesgo relevante de explosión o de causación de otros daños de especial gravedad, o poniendo en peligro la vida o la integridad de las personas.

2. Será castigado con la pena de prisión de tres a cinco años y multa de doce a veinticuatro meses el que cometiere los daños previstos en el apartado 2 del artículo 263, en cualquiera de las circunstancias mencionadas en el apartado anterior.

3. Será castigado con la pena de prisión de cuatro a ocho años el que cometiere los daños previstos en los artículos 265, 323 y 560, en cualquiera de las circunstancias mencionadas en el apartado 1 del presente artículo.

4. En cualquiera de los supuestos previstos en los apartados anteriores, cuando se cometieren los daños concurriendo la provocación de explosiones o la utilización de otros medios de similar potencia destructiva y, además, se pusiera en peligro la vida o integridad de las personas, la pena se impondrá en su mitad superior.

En caso de incendio será de aplicación lo dispuesto en el artículo 351.

Artículo 267.

Los daños causados por imprudencia grave en cuantía superior a 80.000 euros, serán castigados con la pena de multa de tres a nueve meses, atendiendo a la importancia de los mismos.

Las infracciones a que se refiere este artículo sólo serán perseguibles previa denuncia de la persona agraviada o de su representante legal. El Ministerio Fiscal también podrá denunciar cuando aquélla sea menor de edad, persona con discapacidad necesitada de especial protección o una persona desvalida.

En estos casos, el perdón de la persona ofendida extingue la acción penal.

CAPÍTULO X

Disposiciones comunes a los capítulos anteriores

Artículo 268.

1. Están exentos de responsabilidad criminal y sujetos únicamente a la civil los cónyuges que no estuvieren separados legalmente o de hecho o en proceso judicial de separación, divorcio o nulidad de su matrimonio y los ascendientes, descendientes y hermanos por naturaleza o por adopción, así como los afines en primer grado si viviesen juntos, por los delitos patrimoniales que se causaren entre sí, siempre que no concurra violencia o intimidación, o abuso de la vulnerabilidad de la víctima, ya sea por razón de edad, o por tratarse de una persona con discapacidad.

2. Esta disposición no es aplicable a los extraños que participaren en el delito.

Artículo 269.

La provocación, la conspiración y la proposición para cometer los delitos de robo, extorsión, estafa o apropiación indebida, serán castigadas con la pena inferior en uno o dos grados a la del delito correspondiente.

CAPÍTULO XI

De los delitos relativos a la propiedad intelectual e industrial, al mercado y a los consumidores

Sección 1.ª De los delitos relativos a la propiedad intelectual

Artículo 270.

1. Será castigado con la pena de prisión de seis meses a cuatro años y multa de doce a veinticuatro meses el que, con ánimo de obtener un beneficio económico directo o indirecto y en perjuicio de tercero, reproduzca, plagie, distribuya, comunique públicamente o de cualquier otro modo explote económicamente, en todo o en parte, una obra o prestación literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios.

2. La misma pena se impondrá a quien, en la prestación de servicios de la sociedad de la información, con ánimo de obtener un beneficio económico directo o indirecto, y en perjuicio de tercero, facilite de modo activo y no neutral y sin limitarse a un tratamiento meramente técnico, el acceso o la localización en internet de obras o prestaciones objeto de propiedad intelectual sin la autorización de los titulares de los correspondientes derechos o de sus cesionarios, en particular ofreciendo listados ordenados y clasificados de enlaces a las obras y contenidos referidos anteriormente, aunque dichos enlaces hubieran sido facilitados inicialmente por los destinatarios de sus servicios.

3. En estos casos, el juez o tribunal ordenará la retirada de las obras o prestaciones objeto de la infracción. Cuando a través de un portal de acceso a internet o servicio de la sociedad de la información, se difundan exclusiva o preponderantemente los contenidos objeto de la propiedad intelectual a que se refieren los apartados anteriores, se ordenará la interrupción de la prestación del mismo, y el juez podrá acordar cualquier medida cautelar que tenga por objeto la protección de los derechos de propiedad intelectual.

Excepcionalmente, cuando exista reiteración de las conductas y cuando resulte una medida proporcionada, eficiente y eficaz, se podrá ordenar el bloqueo del acceso correspondiente.

4. En los supuestos a que se refiere el apartado 1, la distribución o comercialización ambulante o meramente ocasional se castigará con una pena de prisión de seis meses a dos años.

No obstante, atendidas las características del culpable y la reducida cuantía del beneficio económico obtenido o que se hubiera podido obtener, siempre que no concurra ninguna de

las circunstancias del artículo 271, el Juez podrá imponer la pena de multa de uno a seis meses o trabajos en beneficio de la comunidad de treinta y uno a sesenta días.

5. Serán castigados con las penas previstas en los apartados anteriores, en sus respectivos casos, quienes:

a) Exporten o almacenen intencionadamente ejemplares de las obras, producciones o ejecuciones a que se refieren los dos primeros apartados de este artículo, incluyendo copias digitales de las mismas, sin la referida autorización, cuando estuvieran destinadas a ser reproducidas, distribuidas o comunicadas públicamente.

b) Importen intencionadamente estos productos sin dicha autorización, cuando estuvieran destinados a ser reproducidos, distribuidos o comunicados públicamente, tanto si éstos tienen un origen lícito como ilícito en su país de procedencia; no obstante, la importación de los referidos productos de un Estado perteneciente a la Unión Europea no será punible cuando aquellos se hayan adquirido directamente del titular de los derechos en dicho Estado, o con su consentimiento.

c) Favorezcan o faciliten la realización de las conductas a que se refieren los apartados 1 y 2 de este artículo eliminando o modificando, sin autorización de los titulares de los derechos de propiedad intelectual o de sus cesionarios, las medidas tecnológicas eficaces incorporadas por éstos con la finalidad de impedir o restringir su realización.

d) Con ánimo de obtener un beneficio económico directo o indirecto, con la finalidad de facilitar a terceros el acceso a un ejemplar de una obra literaria, artística o científica, o a su transformación, interpretación o ejecución artística, fijada en cualquier tipo de soporte o comunicado a través de cualquier medio, y sin autorización de los titulares de los derechos de propiedad intelectual o de sus cesionarios, eluda o facilite la elusión de las medidas tecnológicas eficaces dispuestas para evitarlo.

6. Será castigado también con una pena de prisión de seis meses a tres años quien fabrique, importe, ponga en circulación o posea con una finalidad comercial cualquier medio principalmente concebido, producido, adaptado o realizado para facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador o cualquiera de las otras obras, interpretaciones o ejecuciones en los términos previstos en los dos primeros apartados de este artículo.

Artículo 271.

Se impondrá la pena de prisión de dos a seis años, multa de dieciocho a treinta y seis meses e inhabilitación especial para el ejercicio de la profesión relacionada con el delito cometido, por un período de dos a cinco años, cuando se cometa el delito del artículo anterior concurriendo alguna de las siguientes circunstancias:

a) Que el beneficio obtenido o que se hubiera podido obtener posea especial trascendencia económica.

b) Que los hechos revistan especial gravedad, atendiendo el valor de los objetos producidos ilícitamente, el número de obras, o de la transformación, ejecución o interpretación de las mismas, ilícitamente reproducidas, distribuidas, comunicadas al público o puestas a su disposición, o a la especial importancia de los perjuicios ocasionados.

c) Que el culpable perteneciere a una organización o asociación, incluso de carácter transitorio, que tuviese como finalidad la realización de actividades infractoras de derechos de propiedad intelectual.

d) Que se utilice a menores de 18 años para cometer estos delitos.

Artículo 272.

1. La extensión de la responsabilidad civil derivada de los delitos tipificados en los dos artículos anteriores se regirá por las disposiciones de la Ley de Propiedad Intelectual relativas al cese de la actividad ilícita y a la indemnización de daños y perjuicios.

2. En el supuesto de sentencia condenatoria, el Juez o Tribunal podrá decretar la publicación de ésta, a costa del infractor, en un periódico oficial.

Sección 2.ª De los delitos relativos a la propiedad industrial

Artículo 273.

1. Será castigado con la pena de prisión de seis meses a dos años y multa de 12 a 24 meses el que, con fines industriales o comerciales, sin consentimiento del titular de una patente o modelo de utilidad y con conocimiento de su registro, fabrique, importe, posea, utilice, ofrezca o introduzca en el comercio objetos amparados por tales derechos.

2. Las mismas penas se impondrán al que, de igual manera, y para los citados fines, utilice u ofrezca la utilización de un procedimiento objeto de una patente, o posea, ofrezca, introduzca en el comercio, o utilice el producto directamente obtenido por el procedimiento patentado.

3. Será castigado con las mismas penas el que realice cualquiera de los actos tipificados en el párrafo primero de este artículo concurriendo iguales circunstancias en relación con objetos amparados en favor de tercero por un modelo o dibujo industrial o artístico o topografía de un producto semiconductor.

Artículo 274.

1. Será castigado con las penas de uno a cuatro años de prisión y multa de doce a veinticuatro meses el que, con fines industriales o comerciales, sin consentimiento del titular de un derecho de propiedad industrial registrado conforme a la legislación de marcas y con conocimiento del registro,

a) fabrique, produzca o importe productos que incorporen un signo distintivo idéntico o confundible con aquel, u

b) ofrezca, distribuya, o comercialice al por mayor productos que incorporen un signo distintivo idéntico o confundible con aquel, o los almacene con esa finalidad, cuando se trate de los mismos o similares productos, servicios o actividades para los que el derecho de propiedad industrial se encuentre registrado.

2. Será castigado con las penas de seis meses a tres años de prisión el que, con fines industriales o comerciales, sin consentimiento del titular de un derecho de propiedad industrial registrado conforme a la legislación de marcas y con conocimiento del registro, ofrezca, distribuya o comercialice al por menor, o preste servicios o desarrolle actividades, que incorporen un signo distintivo idéntico o confundible con aquél, cuando se trate de los mismos o similares productos, servicios o actividades para los que el derecho de propiedad industrial se encuentre registrado.

La misma pena se impondrá a quien reproduzca o imite un signo distintivo idéntico o confundible con aquél para su utilización para la comisión de las conductas sancionadas en este artículo.

3. La venta ambulante u ocasional de los productos a que se refieren los apartados anteriores será castigada con la pena de prisión de seis meses a dos años.

No obstante, atendidas las características del culpable y la reducida cuantía del beneficio económico obtenido o que se hubiera podido obtener, siempre que no concurra ninguna de las circunstancias del artículo 276, el Juez podrá imponer la pena de multa de uno a seis meses o trabajos en beneficio de la comunidad de treinta y uno a sesenta días.

4. Será castigado con las penas de uno a tres años de prisión el que, con fines agrarios o comerciales, sin consentimiento del titular de un título de obtención vegetal y con conocimiento de su registro, produzca o reproduzca, acondicione con vistas a la producción o reproducción, ofrezca en venta, venda o comercialice de otra forma, exporte o importe, o posea para cualquiera de los fines mencionados, material vegetal de reproducción o multiplicación de una variedad vegetal protegida conforme a la legislación nacional o de la Unión Europea sobre protección de obtenciones vegetales.

Será castigado con la misma pena quien realice cualesquiera de los actos descritos en el párrafo anterior utilizando, bajo la denominación de una variedad vegetal protegida, material vegetal de reproducción o multiplicación que no pertenezca a tal variedad.

Artículo 275.

Las mismas penas previstas en el artículo anterior se impondrán a quien intencionadamente y sin estar autorizado para ello, utilice en el tráfico económico una denominación de origen o una indicación geográfica representativa de una calidad determinada legalmente protegidas para distinguir los productos amparados por ellas, con conocimiento de esta protección.

Artículo 276.

Se impondrá la pena de prisión de dos a seis años, multa de dieciocho a treinta y seis meses e inhabilitación especial para el ejercicio de la profesión relacionada con el delito cometido, por un período de dos a cinco años, cuando concurra alguna de las siguientes circunstancias:

a) Que el beneficio obtenido o que se hubiera podido obtener posea especial trascendencia económica.
b) Que los hechos revistan especial gravedad, atendiendo al valor de los objetos producidos ilícitamente, distribuidos, comercializados u ofrecidos, o a la especial importancia de los perjuicios ocasionados.
c) Que el culpable perteneciere a una organización o asociación, incluso de carácter transitorio, que tuviese como finalidad la realización de actividades infractoras de derechos de propiedad industrial.
d) Que se utilice a menores de 18 años para cometer estos delitos.

Artículo 277.

Será castigado con las penas de prisión de seis meses a dos años y multa de seis a veinticuatro meses, el que intencionadamente haya divulgado la invención objeto de una solicitud de patente secreta, en contravención con lo dispuesto en la legislación de patentes, siempre que ello sea en perjuicio de la defensa nacional.

Sección 3.ª De los delitos relativos al mercado y a los consumidores

Artículo 278.

1. El que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197, será castigado con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses.
2. Se impondrá la pena de prisión de tres a cinco años y multa de doce a veinticuatro meses si se difundieren, revelaren o cedieren a terceros los secretos descubiertos.
3. Lo dispuesto en el presente artículo se entenderá sin perjuicio de las penas que pudieran corresponder por el apoderamiento o destrucción de los soportes informáticos.

Artículo 279.

La difusión, revelación o cesión de un secreto de empresa llevada a cabo por quien tuviere legal o contractualmente obligación de guardar reserva, se castigará con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses.
Si el secreto se utilizara en provecho propio, las penas se impondrán en su mitad inferior.

Artículo 280.

El que, con conocimiento de su origen ilícito, y sin haber tomado parte en su descubrimiento, realizare alguna de las conductas descritas en los dos artículos anteriores, será castigado con la pena de prisión de uno a tres años y multa de doce a veinticuatro meses.

Artículo 281.

1. El que detrajere del mercado materias primas o productos de primera necesidad con la intención de desabastecer un sector del mismo, de forzar una alteración de precios, o de perjudicar gravemente a los consumidores, será castigado con la pena de prisión de uno a cinco años y multa de doce a veinticuatro meses.

2. Se impondrá la pena superior en grado si el hecho se realiza en situaciones de grave necesidad o catastróficas.

Artículo 282.

Serán castigados con la pena de prisión de seis meses a un año o multa de 12 a 24 meses los fabricantes o comerciantes que, en sus ofertas o publicidad de productos o servicios, hagan alegaciones falsas o manifiesten características inciertas sobre los mismos, de modo que puedan causar un perjuicio grave y manifiesto a los consumidores, sin perjuicio de la pena que corresponda aplicar por la comisión de otros delitos.

Artículo 282 bis.

Los que, como administradores de hecho o de derecho de una sociedad emisora de valores negociados en los mercados de valores, falsearan la información económico-financiera contenida en los folletos de emisión de cualesquiera instrumentos financieros o las informaciones que la sociedad debe publicar y difundir conforme a la legislación del mercado de valores sobre sus recursos, actividades y negocios presentes y futuros, con el propósito de captar inversores o depositantes, colocar cualquier tipo de activo financiero, u obtener financiación por cualquier medio, serán castigados con la pena de prisión de uno a cuatro años, sin perjuicio de lo dispuesto en el artículo 308 de este Código.

En el supuesto de que se llegue a obtener la inversión, el depósito, la colocación del activo o la financiación, con perjuicio para el inversor, depositante, adquiriente de los activos financieros o acreedor, se impondrá la pena en la mitad superior. Si el perjuicio causado fuera de notoria gravedad, la pena a imponer será de uno a seis años de prisión y multa de seis a doce meses.

Artículo 283.

Se impondrán las penas de prisión de seis meses a un año y multa de seis a dieciocho meses a los que, en perjuicio del consumidor, facturen cantidades superiores por productos o servicios cuyo costo o precio se mida por aparatos automáticos, mediante la alteración o manipulación de éstos.

Artículo 284.

1. Se impondrá la pena de prisión de seis meses a seis años, multa de dos a cinco años, o del tanto al triplo del beneficio obtenido o favorecido, o de los perjuicios evitados, si la cantidad resultante fuese más elevada, e inhabilitación especial para intervenir en el mercado financiero como actor, agente o mediador o informador por tiempo de dos a cinco años, a los que:

1.º Empleando violencia, amenaza, engaño o cualquier otro artificio, alterasen los precios que hubieren de resultar de la libre concurrencia de productos, mercancías, instrumentos financieros, contratos de contado sobre materias primas relacionadas con ellos, índices de referencia, servicios o cualesquiera otras cosas muebles o inmuebles que sean objeto de contratación, sin perjuicio de la pena que pudiere corresponderles por otros delitos cometidos.

2.º Por sí, de manera directa o indirecta o a través de un medio de comunicación, por medio de internet o mediante el uso de tecnologías de la información y la comunicación, o por cualquier otro medio, difundieren noticias o rumores o transmitieren señales falsas o engañosas sobre personas o empresas, ofreciendo a sabiendas datos económicos total o parcialmente falsos con el fin de alterar o preservar el precio de cotización de un instrumento financiero o un contrato de contado sobre materias primas relacionado o de manipular el

cálculo de un índice de referencia, cuando obtuvieran, para sí o para tercero, un beneficio, siempre que concurra alguna de las siguientes circunstancias:

a) que dicho beneficio fuera superior a doscientos cincuenta mil euros o se causara un perjuicio de idéntica cantidad;
b) que el importe de los fondos empleados fuera superior a dos millones de euros;
c) que se causara un grave impacto en la integridad del mercado.

3.º Realizaren transacciones, transmitieren señales falsas o engañosas, o dieren órdenes de operación susceptibles de proporcionar indicios falsos o engañosos sobre la oferta, la demanda o el precio de un instrumento financiero, un contrato de contado sobre materias primas relacionado o índices de referencia, o se aseguraren, utilizando la misma información, por sí o en concierto con otros, una posición dominante en el mercado de dichos instrumentos o contratos con la finalidad de fijar sus precios en niveles anormales o artificiales, siempre que concurra alguna de las siguientes circunstancias:

a) que como consecuencia de su conducta obtuvieran, para sí o para tercero, un beneficio superior a doscientos cincuenta mil euros o causara un perjuicio de idéntica cantidad;
b) que el importe de los fondos empleados fuera superior a dos millones de euros;
c) que se causara un grave impacto en la integridad del mercado.

2. Se impondrá la pena en su mitad superior si concurriera alguna de las siguientes circunstancias:

1.ª Que el sujeto se dedique de forma habitual a las anteriores prácticas abusivas.
2.ª Que el beneficio obtenido, la pérdida evitada o el perjuicio causado sea de notoria importancia.

3. Si el responsable del hecho fuera trabajador o empleado de una empresa de servicios de inversión, entidad de crédito, autoridad supervisora o reguladora, o entidad rectora de mercados regulados o centros de negociación, las penas se impondrán en su mitad superior.

Artículo 285.

1. Quien de forma directa o indirecta o por persona interpuesta realizare actos de adquisición, transmisión o cesión de un instrumento financiero, o de cancelación o modificación de una orden relativa a un instrumento financiero, utilizando información privilegiada a la que hubiera tenido acceso reservado en los términos del apartado 4, o recomendare a un tercero el uso de dicha información privilegiada para alguno de esos actos, será castigado con la pena de prisión de seis meses a seis años, multa de dos a cinco años, o del tanto al triplo del beneficio obtenido o favorecido o de los perjuicios evitados si la cantidad resultante fuese más elevada, e inhabilitación especial para el ejercicio de la profesión o actividad de dos a cinco años, siempre que concurra alguna de las siguientes circunstancias:

a) que, como consecuencia de su conducta obtuviera, para sí o para tercero, un beneficio superior a quinientos mil euros o causara un perjuicio de idéntica cantidad;
b) que el valor de los instrumentos financieros empleados fuera superior a dos millones de euros;
c) que se causara un grave impacto en la integridad del mercado.

2. Se impondrá la pena en su mitad superior si concurriera alguna de las siguientes circunstancias:

1.ª Que el sujeto se dedique de forma habitual a las anteriores prácticas de operaciones con información privilegiada.
2.ª Que el beneficio obtenido, la pérdida evitada o el perjuicio causado sea de notoria importancia.

3. Las penas previstas en este artículo se impondrán, en sus respectivos casos, en su mitad superior si el responsable del hecho fuera trabajador o empleado de una empresa de

servicios de inversión, entidad de crédito, autoridad supervisora o reguladora, o entidades rectoras de mercados regulados o centros de negociación.

4. A los efectos de este artículo, se entiende que tiene acceso reservado a la información privilegiada quien sea miembro de los órganos de administración, gestión o supervisión del emisor o del participante del mercado de derechos de emisión, quien participe en el capital del emisor o del participante del mercado de derechos de emisión, quien la conozca con ocasión del ejercicio de su actividad profesional o empresarial, o en el desempeño de sus funciones, y quien la obtenga a través de una actividad delictiva.

5. Las mismas penas previstas en este artículo se impondrán cuando el responsable del hecho, sin tener acceso reservado a la información privilegiada, la obtenga de cualquier modo distinto de los previstos en el apartado anterior y la utilice conociendo que se trata de información privilegiada.

Artículo 285 bis.

Fuera de los casos previstos en el artículo anterior, quien poseyera información privilegiada y la revelare fuera del normal ejercicio de su trabajo, profesión o funciones, poniendo en peligro la integridad del mercado o la confianza de los inversores, será sancionado con pena de prisión de seis meses a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para el ejercicio de la profesión o actividad de uno a tres años.

A los efectos de lo dispuesto en este artículo, se incluirá la revelación de información privilegiada en una prospección de mercado cuando se haya realizado sin observar los requisitos previstos en la normativa europea en materia de mercados e instrumentos financieros.

Artículo 285 ter.

Las previsiones de los tres artículos precedentes se extenderán a los instrumentos financieros, contratos, conductas, operaciones y órdenes previstos en la normativa europea y española en materia de mercado e instrumentos financieros.

Artículo 285 quater.

La provocación, la conspiración y la proposición para cometer los delitos previstos en los artículos 284 a 285 bis se castigará, respectivamente, con la pena inferior en uno o dos grados.

Artículo 286.

1. Será castigado con las penas de prisión de seis meses a dos años y multa de seis a 24 meses el que, sin consentimiento del prestador de servicios y con fines comerciales, facilite el acceso inteligible a un servicio de radiodifusión sonora o televisiva, a servicios interactivos prestados a distancia por vía electrónica, o suministre el acceso condicional a los mismos, considerado como servicio independiente, mediante:

1.º La fabricación, importación, distribución, puesta a disposición por vía electrónica, venta, alquiler, o posesión de cualquier equipo o programa informático, no autorizado en otro Estado miembro de la Unión Europea, diseñado o adaptado para hacer posible dicho acceso.

2.º La instalación, mantenimiento o sustitución de los equipos o programas informáticos mencionados en el párrafo 1.º

2. Con idéntica pena será castigado quien, con ánimo de lucro, altere o duplique el número identificativo de equipos de telecomunicaciones, o comercialice equipos que hayan sufrido alteración fraudulenta.

3. A quien, sin ánimo de lucro, facilite a terceros el acceso descrito en el apartado 1, o por medio de una comunicación pública, comercial o no, suministre información a una pluralidad de personas sobre el modo de conseguir el acceso no autorizado a un servicio o el uso de un dispositivo o programa, de los expresados en ese mismo apartado 1, incitando a lograrlos, se le impondrá la pena de multa en él prevista.

4. A quien utilice los equipos o programas que permitan el acceso no autorizado a servicios de acceso condicional o equipos de telecomunicación, se le impondrá la pena prevista en el artículo 255 de este Código con independencia de la cuantía de la defraudación.

Sección 4.ª Delitos de corrupción en los negocios

Artículo 286 bis.

1. El directivo, administrador, empleado o colaborador de una empresa mercantil o de una sociedad que, por sí o por persona interpuesta, reciba, solicite o acepte un beneficio o ventaja no justificados de cualquier naturaleza, u ofrecimiento o promesa de obtenerlo, para sí o para un tercero, como contraprestación para favorecer indebidamente a otro en la adquisición o venta de mercancías, o en la contratación de servicios o en las relaciones comerciales, será castigado con la pena de prisión de seis meses a cuatro años, inhabilitación especial para el ejercicio de industria o comercio por tiempo de uno a seis años y multa del tanto al triplo del valor del beneficio o ventaja.

2. Con las mismas penas será castigado quien, por sí o por persona interpuesta, prometa, ofrezca o conceda a directivos, administradores, empleados o colaboradores de una empresa mercantil o de una sociedad, un beneficio o ventaja no justificados, de cualquier naturaleza, para ellos o para terceros, como contraprestación para que le favorezca indebidamente a él o a un tercero frente a otros en la adquisición o venta de mercancías, contratación de servicios o en las relaciones comerciales.

3. Los jueces y tribunales, en atención a la cuantía del beneficio o al valor de la ventaja, y a la trascendencia de las funciones del culpable, podrán imponer la pena inferior en grado y reducir la de multa a su prudente arbitrio.

4. Lo dispuesto en este artículo será aplicable, en sus respectivos casos, a los directivos, administradores, empleados o colaboradores de una entidad deportiva, cualquiera que sea la forma jurídica de ésta, así como a los deportistas, árbitros o jueces, respecto de aquellas conductas que tengan por finalidad predeterminar o alterar de manera deliberada y fraudulenta el resultado de una prueba, encuentro o competición deportiva de especial relevancia económica o deportiva.

A estos efectos, se considerará competición deportiva de especial relevancia económica, aquélla en la que la mayor parte de los participantes en la misma perciban cualquier tipo de retribución, compensación o ingreso económico por su participación en la actividad; y competición deportiva de especial relevancia deportiva, la que sea calificada en el calendario deportivo anual aprobado por la federación deportiva correspondiente como competición oficial de la máxima categoría de la modalidad, especialidad, o disciplina de que se trate.

5. A los efectos de este artículo resulta aplicable lo dispuesto en el artículo 297.

Artículo 286 ter.

1. Los que mediante el ofrecimiento, promesa o concesión de cualquier beneficio o ventaja indebidos, pecuniarios o de otra clase, corrompieren o intentaren corromper, por sí o por persona interpuesta, a una autoridad o funcionario público en beneficio de estos o de un tercero, o atendieran sus solicitudes al respecto, con el fin de que actúen o se abstengan de actuar en relación con el ejercicio de funciones públicas para conseguir o conservar un contrato, negocio o cualquier otra ventaja competitiva en la realización de actividades económicas internacionales, serán castigados, salvo que ya lo estuvieran con una pena más grave en otro precepto de este Código, con las penas de prisión de prisión de tres a seis años, multa de doce a veinticuatro meses, salvo que el beneficio obtenido fuese superior a la cantidad resultante, en cuyo caso la multa será del tanto al triplo del montante de dicho beneficio.

Además de las penas señaladas, se impondrá en todo caso al responsable la pena de prohibición de contratar con el sector público, así como la pérdida de la posibilidad de obtener subvenciones o ayudas públicas y del derecho a gozar de beneficios o incentivos fiscales y de la Seguridad Social, y la prohibición de intervenir en transacciones comerciales de trascendencia pública por un periodo de siete a doce años.

2. A los efectos de este artículo se entenderá por funcionario público los determinados por los artículos 24 y 427.

Artículo 286 quater.

Si los hechos a que se refieren los artículos de esta Sección resultaran de especial gravedad, se impondrá la pena en su mitad superior, pudiéndose llegar hasta la superior en grado.

Los hechos se considerarán, en todo caso, de especial gravedad cuando:

a) el beneficio o ventaja tenga un valor especialmente elevado,

b) la acción del autor no sea meramente ocasional,

c) se trate de hechos cometidos en el seno de una organización o grupo criminal, o

d) el objeto del negocio versara sobre bienes o servicios humanitarios o cualesquiera otros de primera necesidad.

En el caso del apartado 4 del artículo 286 bis, los hechos se considerarán también de especial gravedad cuando:

a) tengan como finalidad influir en el desarrollo de juegos de azar o apuestas; o

b) sean cometidos en una competición deportiva oficial de ámbito estatal calificada como profesional o en una competición deportiva internacional.

[. . .]

TÍTULO XVI BIS

De los delitos contra los animales

Artículo 340 bis.

1. Será castigado con la pena de prisión de tres a dieciocho meses o multa de seis a doce meses y con la pena de inhabilitación especial de uno a tres años para el ejercicio de profesión, oficio o comercio que tenga relación con los animales y para la tenencia de animales el que fuera de las actividades legalmente reguladas y por cualquier medio o procedimiento, incluyendo los actos de carácter sexual, cause a un animal doméstico, amansado, domesticado o que viva temporal o permanentemente bajo el control humano lesión que requiera tratamiento veterinario para el restablecimiento de su salud.

Si las lesiones del apartado anterior se causaren a un animal vertebrado no incluido en el apartado anterior, se impondrá la pena de prisión de tres a doce meses o multa de tres a seis meses, además de la pena de inhabilitación especial de uno a tres años para el ejercicio de la profesión, oficio o comercio que tenga relación con los animales y para la tenencia de animales.

Si el delito se hubiera cometido utilizando armas de fuego, el juez o tribunal podrá imponer motivadamente la pena de privación del derecho a tenencia y porte de armas por un tiempo de uno a cuatro años.

2. Las penas previstas en el apartado anterior se impondrán en su mitad superior cuando concurra alguna de las siguientes circunstancias agravantes:

a) Utilizar armas, instrumentos, objetos, medios, métodos o formas que pudieran resultar peligrosas para la vida o salud del animal.

b) Ejecutar el hecho con ensañamiento.

c) Causar al animal la pérdida o la inutilidad de un sentido, órgano o miembro principal.

d) Realizar el hecho por su propietario o quien tenga confiado el cuidado del animal.

e) Ejecutar el hecho en presencia de un menor de edad o de una persona especialmente vulnerable.

f) Ejecutar el hecho con ánimo de lucro.

g) Cometer el hecho para coaccionar, intimidar, acosar o producir menoscabo psíquico a quien sea o haya sido cónyuge o a persona que esté o haya estado ligada al autor por una análoga relación de afectividad, aun sin convivencia.

h) Ejecutar el hecho en un evento público o difundirlo a través de tecnologías de la información o la comunicación.

i) Utilizar veneno, medios explosivos u otros instrumentos o artes de similar eficacia destructiva o no selectiva.

3. Cuando, con ocasión de los hechos previstos en el apartado primero de este artículo, se cause la muerte de un animal doméstico, amansado, domesticado o que viva temporal o permanentemente bajo el control humano, se impondrá la pena de prisión de doce a veinticuatro meses, además de la pena de inhabilitación especial de dos a cuatro años para el ejercicio de profesión, oficio o comercio que tenga relación con los animales y para la tenencia de animales.

Cuando, con ocasión de los hechos previstos en el apartado primero de este artículo, se cause muerte de un animal vertebrado no incluido en el apartado anterior, se impondrá la pena de prisión de seis a dieciocho meses o multa de dieciocho a veinticuatro meses, además de la pena de inhabilitación especial de dos a cuatro años para el ejercicio de la profesión, oficio o comercio que tenga relación con los animales y para la tenencia de animales.

Si el delito se hubiera cometido utilizando armas de fuego, el juez o tribunal podrá imponer motivadamente la pena de privación del derecho a tenencia y porte de armas por un tiempo de dos a cinco años.

Cuando concurra alguna de las circunstancias previstas en el apartado anterior, el juez o tribunal impondrá las penas en su mitad superior.

4. Si las lesiones producidas no requiriesen tratamiento veterinario o se hubiere maltratado gravemente al animal sin causarle lesiones, se impondrá una pena de multa de uno a dos meses o trabajos en beneficio de la comunidad de uno a treinta días. Asimismo, se impondrá la pena de inhabilitación especial de tres meses a un año para el ejercicio de profesión, oficio o comercio que tenga relación con los animales y para la tenencia de animales.

Artículo 340 ter.

Quien abandone a un animal vertebrado que se encuentre bajo su responsabilidad en condiciones en que pueda peligrar su vida o integridad será castigado con una pena de multa de uno a seis meses o de trabajos en beneficio de la comunidad de treinta y uno a noventa días. Asimismo, se impondrá la pena de inhabilitación especial de uno a tres años para el ejercicio de profesión, oficio o comercio que tenga relación con los animales y para la tenencia de animales.

Artículo 340 quater.

1. Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos recogidos en este título, se le impondrán las siguientes penas:

a) Multa de uno a tres años, si el delito cometido por la persona física tiene prevista en la ley una pena de prisión superior a dos años.

b) Multa de seis meses a dos años, en el resto de los casos.

2. Atendidas las reglas establecidas en el artículo 66 bis, en los supuestos de responsabilidad de personas jurídicas los jueces y tribunales podrán asimismo imponer las penas recogidas en el artículo 33.7, párrafos b) a g).

Artículo 340 quinquies.

Los jueces o tribunales podrán adoptar motivadamente cualquier medida cautelar necesaria para la protección de los bienes tutelados en este Título, incluyendo cambios provisionales sobre la titularidad y cuidado del animal.

Cuando la pena de inhabilitación especial para el ejercicio de profesión, oficio o comercio que tenga relación con los animales y para la tenencia de animales recaiga sobre la persona que tuviera a asignada la titularidad o cuidado del animal maltratado, el juez o tribunal, de

oficio o a instancia de parte, adoptará las medidas pertinentes respecto a la titularidad y el cuidado del animal.

[. . .]

TÍTULO XVIII

De las falsedades

[. . .]

CAPÍTULO IV

De la usurpación del estado civil

Artículo 401.

El que usurpare el estado civil de otro será castigado con la pena de prisión de seis meses a tres años.

[. . .]

CAPÍTULO III

Del descubrimiento y revelación de secretos e informaciones relativas a la Defensa Nacional

Artículo 598.

El que, sin propósito de favorecer a una potencia extranjera, se procurare, revelare, falseare o inutilizare información legalmente calificada como reservada o secreta, relacionada con la seguridad nacional o la defensa nacional o relativa a los medios técnicos o sistemas empleados por las Fuerzas Armadas o las industrias de interés militar, será castigado con la pena de prisión de uno a cuatro años.

Artículo 599.

La pena establecida en el artículo anterior se aplicará en su mitad superior cuando concurra alguna de las circunstancias siguientes:

1.º Que el sujeto activo sea depositario o conocedor del secreto o información por razón de su cargo o destino.

2.º Que la revelación consistiera en dar publicidad al secreto o información en algún medio de comunicación social o de forma que asegure su difusión.

Artículo 600.

1. El que sin autorización expresa reprodujere planos o documentación referentes a zonas, instalaciones o materiales militares que sean de acceso restringido y cuyo conocimiento esté protegido y reservado por una información legalmente calificada como reservada o secreta, será castigado con la pena de prisión de seis meses a tres años.

2. Con la misma pena será castigado el que tenga en su poder objetos o información legalmente calificada como reservada o secreta, relativos a la seguridad o a la defensa nacional, sin cumplir las disposiciones establecidas en la legislación vigente.

Artículo 601.

El que, por razón de su cargo, comisión o servicio, tenga en su poder o conozca oficialmente objetos o información legalmente calificada como reservada o secreta o de interés militar, relativos a la seguridad nacional o la defensa nacional, y por imprudencia grave dé lugar a que sean conocidos por persona no autorizada o divulgados, publicados o inutilizados, será castigado con la pena de prisión de seis meses a un año.

Artículo 602.

El que descubriere, violare, revelare, sustrajere o utilizare información legalmente calificada como reservada o secreta relacionada con la energía nuclear, será castigado con la pena de prisión de seis meses a tres años, salvo que el hecho tenga señalada pena más grave en otra Ley.

Artículo 603.

El que destruyere, inutilizare, falseare o abriere sin autorización la correspondencia o documentación legalmente calificada como reservada o secreta, relacionadas con la defensa nacional y que tenga en su poder por razones de su cargo o destino, será castigado con la pena de prisión de dos a cinco años e inhabilitación especial de empleo o cargo público por tiempo de tres a seis años.

[. . .]

§ 49

Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 11, de 13 de enero de 2000
Última modificación: 3 de enero de 2025
Referencia: BOE-A-2000-641

TÍTULO PRELIMINAR

Artículo 1. *Declaración general.*

1. Esta Ley se aplicará para exigir la responsabilidad de las personas mayores de catorce años y menores de dieciocho por la comisión de hechos tipificados como delitos o faltas en el Código Penal o las leyes penales especiales.

2. Las personas a las que se aplique la presente Ley gozarán de todos los derechos reconocidos en la Constitución y en el ordenamiento jurídico, particularmente en la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, así como en la Convención sobre los Derechos del Niño de 20 de noviembre de 1989 y en todas aquellas normas sobre protección de menores contenidas en los Tratados válidamente celebrados por España.

TÍTULO I

Del ámbito de aplicación de la Ley

Artículo 2. *Competencia de los Jueces de Menores.*

1. Los Jueces de Menores serán competentes para conocer de los hechos cometidos por las personas mencionadas en el artículo 1 de esta Ley, así como para hacer ejecutar las sentencias, sin perjuicio de las facultades atribuidas por esta Ley a las Comunidades Autónomas respecto a la protección y reforma de menores.

2. Los Jueces de Menores serán asimismo competentes para resolver sobre las responsabilidades civiles derivadas de los hechos cometidos por las personas a las que resulta aplicable la presente Ley.

3. La competencia corresponde al Juez de Menores del lugar donde se haya cometido el hecho delictivo, sin perjuicio de lo establecido en el artículo 20.3 de esta Ley.

4. La competencia para conocer de los delitos previstos en los artículos 571 a 580 del Código Penal corresponderá al Juzgado Central de Menores de la Audiencia Nacional.

Corresponderá igualmente al Juzgado Central de Menores de la Audiencia Nacional la competencia para conocer de los delitos cometidos por menores en el extranjero cuando

conforme al artículo 23 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial y a los Tratados Internacionales corresponda su conocimiento a la jurisdicción española.

La referencia del último inciso del apartado 4 del artículo 17 y cuantas otras se contienen en la presente Ley al Juez de Menores se entenderán hechas al Juez Central de Menores en lo que afecta a los menores imputados por cualquiera de los delitos a que se refieren los dos párrafos anteriores.

Artículo 3. *Régimen de los menores de catorce años.*

Cuando el autor de los hechos mencionados en los artículos anteriores sea menor de catorce años, no se le exigirá responsabilidad con arreglo a la presente Ley, sino que se le aplicará lo dispuesto en las normas sobre protección de menores previstas en el Código Civil y demás disposiciones vigentes. El Ministerio Fiscal deberá remitir a la entidad pública de protección de menores testimonio de los particulares que considere precisos respecto al menor, a fin de valorar su situación, y dicha entidad habrá de promover las medidas de protección adecuadas a las circunstancias de aquél conforme a lo dispuesto en la Ley Orgánica 1/1996, de 15 de enero.

Artículo 4. *Derechos de las víctimas y de las personas perjudicadas.*

El Ministerio Fiscal y el Juez de Menores velarán en todo momento por la protección de los derechos de las víctimas y de las personas perjudicadas por las infracciones cometidas por las personas menores de edad.

De manera inmediata se les instruirá de las medidas de asistencia a las víctimas que prevé la legislación vigente, debiendo el Letrado de la Administración de Justicia derivar a la víctima de violencia a la Oficina de Atención a la Víctima competente.

Las víctimas y las personas perjudicadas tendrán derecho a personarse y ser parte en el expediente que se incoe al efecto, para lo cual el Letrado de la Administración de Justicia les informará en los términos previstos en los artículos 109 y 110 de la Ley de Enjuiciamiento Criminal, instruyéndoles de su derecho a nombrar dirección letrada o instar su nombramiento de oficio en caso de ser titulares del derecho a la asistencia jurídica gratuita. Asimismo, les informará de que, de no personarse en el expediente y no hacer renuncia ni reserva de acciones civiles, el Ministerio Fiscal las ejercitará si correspondiere.

Se garantizará especialmente que las declaraciones o interrogatorios de las partes acusadoras, testigos o peritos se realicen de forma telemática en los siguientes supuestos, salvo que el Juez, Tribunal o Ministerio Fiscal, mediante resolución motivada, en atención a las circunstancias del caso concreto, estime necesaria su presencia física:

Cuando sean víctimas de violencia de género, de violencia sexual, de trata de seres humanos o cuando sean víctimas menores de edad o con discapacidad. Todas ellas podrán intervenir desde los lugares donde se encuentren recibiendo oficialmente asistencia, atención, asesoramiento o protección, o desde cualquier otro lugar, siempre que dispongan de medios suficientes para asegurar su identidad y las adecuadas condiciones de la intervención.

Téngase en cuenta que este artículo, modificado por el art. 23.1 de la Ley Orgánica 1/2025, de 2 de enero, Ref. BOE-A-2025-76, entra en vigor el 3 de abril de 2025, según determina su disposición final 38.1.

Redacción anterior:

"Artículo 4. Derechos de las víctimas y de las personas perjudicadas.

El Ministerio Fiscal y el Juez de Menores velarán en todo momento por la protección de los derechos de las víctimas y de las personas perjudicadas por las infracciones cometidas por las personas menores de edad.

De manera inmediata se les instruirá de las medidas de asistencia a las víctimas que prevé la legislación vigente, debiendo el Letrado de la Administración de Justicia derivar a la víctima de violencia a la Oficina de Atención a la Víctima competente.

Las víctimas y las personas perjudicadas tendrán derecho a personarse y ser parte en el expediente que se incoe al efecto, para lo cual el Letrado de la Administración de Justicia les informará en los términos previstos en los artículos 109 y 110 de la Ley de Enjuiciamiento Criminal, instruyéndoles de su derecho a nombrar dirección letrada o instar su nombramiento de oficio en caso de ser titulares del derecho a la asistencia jurídica gratuita. Asimismo, les informará de que, de no personarse en el expediente y no hacer renuncia ni reserva de acciones civiles, el Ministerio Fiscal las ejercitará si correspondiere.

Quienes se personaren podrán desde entonces tomar conocimiento de lo actuado e instar la práctica de diligencias y cuanto a su derecho convenga. Sin perjuicio de lo anterior, el Letrado de la Administración de Justicia deberá comunicar a las víctimas y a las personas perjudicadas, se hayan o no personado, todas aquellas resoluciones que se adopten tanto por el Ministerio Fiscal como por el Juez de Menores, que puedan afectar a sus intereses.

En especial, cuando el Ministerio Fiscal, en aplicación de lo dispuesto en el artículo 18 de esta Ley, desista de la incoación del expediente deberá inmediatamente ponerlo en conocimiento de las víctimas y las personas perjudicadas haciéndoles saber su derecho a ejercitar las acciones civiles que les asisten ante la jurisdicción civil.

Del mismo modo, el Letrado de la Administración de Justicia notificará por escrito la sentencia que se dicte a las víctimas y las personas perjudicadas por la infracción penal, aunque no se hayan mostrado parte en el expediente.

Cuando la víctima lo sea de un delito de violencia de género, tiene derecho a que le sean notificadas por escrito, mediante testimonio íntegro, las medidas cautelares de protección adoptadas. Asimismo, tales medidas cautelares serán comunicadas a las administraciones públicas competentes para la adopción de medidas de protección, sean estas de seguridad o de asistencia social, jurídica, sanitaria, psicológica o de cualquier otra índole.

La víctima de un delito violento tiene derecho a ser informada permanentemente de la situación procesal del presunto agresor. En particular, en el caso de una medida, cautelar o definitiva, de internamiento, la víctima será informada en todo momento de los permisos y salidas del centro del presunto agresor, salvo en aquellos casos en los que manifieste su deseo de no recibir notificaciones."

Artículo 5. *Bases de la responsabilidad de los menores.*

1. Los menores serán responsables con arreglo a esta Ley cuando hayan cometido los hechos a los que se refiere el artículo 1 y no concurra en ellos ninguna de las causas de exención o extinción de la responsabilidad criminal previstas en el vigente Código Penal.

2. No obstante lo anterior, a los menores en quienes concurran las circunstancias previstas en los números 1.º, 2.º y 3.º del artículo 20 del vigente Código Penal les serán aplicables, en caso necesario, las medidas terapéuticas a las que se refiere el artículo 7.1, letras d) y e), de la presente Ley.

3. Las edades indicadas en el articulado de esta Ley se han de entender siempre referidas al momento de la comisión de los hechos, sin que el haberse rebasado las mismas antes del comienzo del procedimiento o durante la tramitación del mismo tenga incidencia alguna sobre la competencia atribuida por esta misma Ley a los Jueces y Fiscales de Menores.

Artículo 6. *De la intervención del Ministerio Fiscal.*

Corresponde al Ministerio Fiscal la defensa de los derechos que a los menores reconocen las leyes, así como la vigilancia de las actuaciones que deban efectuarse en su interés y la observancia de las garantías del procedimiento, para lo cual dirigirá personalmente la investigación de los hechos y ordenará que la policía judicial practique las actuaciones necesarias para la comprobación de aquéllos y de la participación del menor en los mismos, impulsando el procedimiento.

TÍTULO II

De las medidas

Artículo 7. *Definición de las medidas susceptibles de ser impuestas a los menores y reglas generales de determinación de las mismas.*

1. Las medidas que pueden imponer los Jueces de Menores, ordenadas según la restricción de derechos que suponen, son las siguientes:

a) Internamiento en régimen cerrado. Las personas sometidas a esta medida residirán en el centro y desarrollarán en el mismo las actividades formativas, educativas, laborales y de ocio.

b) Internamiento en régimen semiabierto. Las personas sometidas a esta medida residirán en el centro, pero podrán realizar fuera del mismo alguna o algunas de las actividades formativas, educativas, laborales y de ocio establecidas en el programa individualizado de ejecución de la medida. La realización de actividades fuera del centro quedará condicionada a la evolución de la persona y al cumplimiento de los objetivos previstos en las mismas, pudiendo el Juez de Menores suspenderlas por tiempo determinado, acordando que todas las actividades se lleven a cabo dentro del centro.

c) Internamiento en régimen abierto. Las personas sometidas a esta medida llevarán a cabo todas las actividades del proyecto educativo en los servicios normalizados del entorno, residiendo en el centro como domicilio habitual, con sujeción al programa y régimen interno del mismo.

d) Internamiento terapéutico en régimen cerrado, semiabierto o abierto. En los centros de esta naturaleza se realizará una atención educativa especializada o tratamiento específico dirigido a personas que padezcan anomalías o alteraciones psíquicas, un estado de dependencia de bebidas alcohólicas, drogas tóxicas o sustancias psicotrópicas, o alteraciones en la percepción que determinen una alteración grave de la conciencia de la realidad. Esta medida podrá aplicarse sola o como complemento de otra medida prevista en este artículo. Cuando el interesado rechace un tratamiento de deshabituación, el Juez habrá de aplicarle otra medida adecuada a sus circunstancias.

e) Tratamiento ambulatorio. Las personas sometidas a esta medida habrán de asistir al centro designado con la periodicidad requerida por los facultativos que las atiendan y seguir las pautas fijadas para el adecuado tratamiento de la anomalía o alteración psíquica, adicción al consumo de bebidas alcohólicas, drogas tóxicas o sustancias psicotrópicas, o alteraciones en la percepción que padezcan. Esta medida podrá aplicarse sola o como complemento de otra medida prevista en este artículo. Cuando el interesado rechace un tratamiento de deshabituación, el Juez habrá de aplicarle otra medida adecuada a sus circunstancias.

f) Asistencia a un centro de día. Las personas sometidas a esta medida residirán en su domicilio habitual y acudirán a un centro, plenamente integrado en la comunidad, a realizar actividades de apoyo, educativas, formativas, laborales o de ocio.

g) Permanencia de fin de semana. Las personas sometidas a esta medida permanecerán en su domicilio o en un centro hasta un máximo de treinta y seis horas entre la tarde o noche del viernes y la noche del domingo, a excepción, en su caso, del tiempo que deban dedicar a las tareas socio-educativas asignadas por el Juez que deban llevarse a cabo fuera del lugar de permanencia.

h) Libertad vigilada. En esta medida se ha de hacer un seguimiento de la actividad de la persona sometida a la misma y de su asistencia a la escuela, al centro de formación profesional o al lugar de trabajo, según los casos, procurando ayudar a aquélla a superar los factores que determinaron la infracción cometida. Asimismo, esta medida obliga, en su caso, a seguir las pautas socio-educativas que señale la entidad pública o el profesional encargado de su seguimiento, de acuerdo con el programa de intervención elaborado al efecto y aprobado por el Juez de Menores. La persona sometida a la medida también queda obligada a mantener con dicho profesional las entrevistas establecidas en el programa y a cumplir, en su caso, las reglas de conducta impuestas por el Juez, que podrán ser alguna o algunas de las siguientes:

1.ª Obligación de asistir con regularidad al centro docente correspondiente, si el menor está en edad de escolarización obligatoria, y acreditar ante el Juez dicha asistencia regular o justificar en su caso las ausencias, cuantas veces fuere requerido para ello.

2.ª Obligación de someterse a programas de tipo formativo, cultural, educativo, profesional, laboral, de educación sexual, de educación vial u otros similares.

3.ª Prohibición de acudir a determinados lugares, establecimientos o espectáculos.

4.ª Prohibición de ausentarse del lugar de residencia sin autorización judicial previa.

5.ª Obligación de residir en un lugar determinado.

6.ª Obligación de comparecer personalmente ante el Juzgado de Menores o profesional que se designe, para informar de las actividades realizadas y justificarlas.

7.ª Cualesquiera otras obligaciones que el Juez, de oficio o a instancia del Ministerio Fiscal, estime convenientes para la reinserción social del sentenciado, siempre que no atenten contra su dignidad como persona. Si alguna de estas obligaciones implicase la imposibilidad del menor de continuar conviviendo con sus padres, tutores o guardadores, el Ministerio Fiscal deberá remitir testimonio de los particulares a la entidad pública de protección del menor, y dicha entidad deberá promover las medidas de protección adecuadas a las circunstancias de aquél, conforme a lo dispuesto en la Ley Orgánica 1/1996.

i) La prohibición de aproximarse o comunicarse con la víctima o con aquellos de sus familiares u otras personas que determine el Juez. Esta medida impedirá al menor acercarse a ellos, en cualquier lugar donde se encuentren, así como a su domicilio, a su centro docente, a sus lugares de trabajo y a cualquier otro que sea frecuentado por ellos. La prohibición de comunicarse con la víctima, o con aquellos de sus familiares u otras personas que determine el Juez o Tribunal, impedirá al menor establecer con ellas, por cualquier medio de comunicación o medio informático o telemático, contacto escrito, verbal o visual. Si esta medida implicase la imposibilidad del menor de continuar viviendo con sus padres, tutores o guardadores, el Ministerio Fiscal deberá remitir testimonio de los particulares a la entidad pública de protección del menor, y dicha entidad deberá promover las medidas de protección adecuadas a las circunstancias de aquél, conforme a lo dispuesto en la Ley Orgánica 1/1996.

j) Convivencia con otra persona, familia o grupo educativo. La persona sometida a esta medida debe convivir, durante el período de tiempo establecido por el Juez, con otra persona, con una familia distinta a la suya o con un grupo educativo, adecuadamente seleccionados para orientar a aquélla en su proceso de socialización.

k) Prestaciones en beneficio de la comunidad. La persona sometida a esta medida, que no podrá imponerse sin su consentimiento, ha de realizar las actividades no retribuidas que se le indiquen, de interés social o en beneficio de personas en situación de precariedad.

l) Realización de tareas socio-educativas. La persona sometida a esta medida ha de realizar, sin internamiento ni libertad vigilada, actividades específicas de contenido educativo encaminadas a facilitarle el desarrollo de su competencia social.

m) Amonestación. Esta medida consiste en la reprensión de la persona llevada a cabo por el Juez de Menores y dirigida a hacerle comprender la gravedad de los hechos cometidos y las consecuencias que los mismos han tenido o podrían haber tenido, instándole a no volver a cometer tales hechos en el futuro.

n) Privación del permiso de conducir ciclomotores y vehículos a motor, o del derecho a obtenerlo, o de las licencias administrativas para caza o para uso de cualquier tipo de armas. Esta medida podrá imponerse como accesoria cuando el delito o falta se hubiere cometido utilizando un ciclomotor o un vehículo a motor, o un arma, respectivamente.

ñ) Inhabilitación absoluta. La medida de inhabilitación absoluta produce la privación definitiva de todos los honores, empleos y cargos públicos sobre el que recayere, aunque sean electivos; así como la incapacidad para obtener los mismos o cualesquiera otros honores, cargos o empleos públicos, y la de ser elegido para cargo público, durante el tiempo de la medida.

2. Las medidas de internamiento constarán de dos períodos: el primero se llevará a cabo en el centro correspondiente, conforme a la descripción efectuada en el apartado anterior de este artículo, el segundo se llevará a cabo en régimen de libertad vigilada, en la modalidad

elegida por el Juez. La duración total no excederá del tiempo que se expresa en los artículos 9 y 10. El equipo técnico deberá informar respecto del contenido de ambos períodos, y el Juez expresará la duración de cada uno en la sentencia.

3. Para la elección de la medida o medidas adecuadas se deberá atender de modo flexible, no sólo a la prueba y valoración jurídica de los hechos, sino especialmente a la edad, las circunstancias familiares y sociales, la personalidad y el interés del menor, puestos de manifiesto los dos últimos en los informes de los equipos técnicos y de las entidades públicas de protección y reforma de menores cuando éstas hubieran tenido conocimiento del menor por haber ejecutado una medida cautelar o definitiva con anterioridad, conforme a lo dispuesto en el artículo 27 de la presente Ley. El Juez deberá motivar en la sentencia las razones por las que aplica una determinada medida, así como el plazo de duración de la misma, a los efectos de la valoración del mencionado interés del menor.

4. El Juez podrá imponer al menor una o varias medidas de las previstas en esta Ley con independencia de que se trate de uno o más hechos, sujetándose si procede a lo dispuesto en el artículo 11 para el enjuiciamiento conjunto de varias infracciones; pero, en ningún caso, se impondrá a un menor en una misma resolución más de una medida de la misma clase, entendiendo por tal cada una de las que se enumeran en el apartado 1 de este artículo.

5. Cuando la medida impuesta lo sea por la comisión de un delito de los previstos en los Capítulos I y II del Título VIII del Código Penal, el Juez impondrá de forma accesoria, en todo caso, la obligación de someterse a programas formativos de educación sexual y de educación en igualdad.

Artículo 8. *Principio acusatorio.*

El Juez de Menores no podrá imponer una medida que suponga una mayor restricción de derechos ni por un tiempo superior a la medida solicitada por el Ministerio Fiscal o por el acusador particular.

Tampoco podrá exceder la duración de las medidas privativas de libertad contempladas en el artículo 7.1.ª), b), c), d) y g), en ningún caso, del tiempo que hubiera durado la pena privativa de libertad que se le hubiere impuesto por el mismo hecho, si el sujeto, de haber sido mayor de edad, hubiera sido declarado responsable, de acuerdo con el Código Penal.

Artículo 9. *Régimen general de aplicación y duración de las medidas.*

No obstante lo establecido en los apartados 3 y 4 del artículo 7, la aplicación de las medidas se atendrá a las siguientes reglas:

1. Cuando los hechos cometidos sean calificados de falta, sólo se podrán imponer las medidas de libertad vigilada hasta un máximo de seis meses, amonestación, permanencia de fin de semana hasta un máximo de cuatro fines de semana, prestaciones en beneficio de la comunidad hasta cincuenta horas, privación del permiso de conducir o de otras licencias administrativas hasta un año, la prohibición de aproximarse o comunicarse con la víctima o con aquellos de sus familiares u otras personas que determine el Juez hasta seis meses, y la realización de tareas socio-educativas hasta seis meses.

2. La medida de internamiento en régimen cerrado sólo podrá ser aplicable cuando:

a) Los hechos estén tipificados como delito grave por el Código Penal o las leyes penales especiales.

b) Tratándose de hechos tipificados como delito menos grave, en su ejecución se haya empleado violencia o intimidación en las personas o se haya generado grave riesgo para la vida o la integridad física de las mismas.

c) Los hechos tipificados como delito se cometan en grupo o el menor perteneciere o actuare al servicio de una banda, organización o asociación, incluso de carácter transitorio, que se dedicare a la realización de tales actividades.

3. La duración de las medidas no podrá exceder de dos años, computándose, en su caso, a estos efectos el tiempo ya cumplido por el menor en medida cautelar, conforme a lo dispuesto en el artículo 28.5 de la presente Ley. La medida de prestaciones en beneficio de la comunidad no podrá superar las cien horas. La medida de permanencia de fin de semana no podrá superar los ocho fines de semana.

4. Las acciones u omisiones imprudentes no podrán ser sancionadas con medidas de internamiento en régimen cerrado.

5. Cuando en la postulación del Ministerio Fiscal o en la resolución dictada en el procedimiento se aprecien algunas de las circunstancias a las que se refiere el artículo 5.2 de esta Ley, sólo podrán aplicarse las medidas terapéuticas descritas en el artículo 7.1, letras d) y e) de la misma.

Artículo 10. *Reglas especiales de aplicación y duración de las medidas.*

1. Cuando se trate de los hechos previstos en el apartado 2 del artículo anterior, el Juez, oído el Ministerio Fiscal, las partes personadas y el equipo técnico, actuará conforme a las reglas siguientes:

a) si al tiempo de cometer los hechos el menor tuviere catorce o quince años de edad, la medida podrá alcanzar tres años de duración. Si se trata de prestaciones en beneficio de la comunidad, dicho máximo será de ciento cincuenta horas, y de doce fines de semana si la medida impuesta fuere la de permanencia de fin de semana.

b) si al tiempo de cometer los hechos el menor tuviere dieciséis o diecisiete años de edad, la duración máxima de la medida será de seis años; o, en sus respectivos casos, de doscientas horas de prestaciones en beneficio de la comunidad o permanencia de dieciséis fines de semana. En este supuesto, cuando el hecho revista extrema gravedad, el Juez deberá imponer una medida de internamiento en régimen cerrado de uno a seis años, complementada sucesivamente con otra medida de libertad vigilada con asistencia educativa hasta un máximo de cinco años. Sólo podrá hacerse uso de lo dispuesto en los artículos 13 y 51.1 de esta Ley Orgánica una vez transcurrido el primer año de cumplimiento efectivo de la medida de internamiento. A los efectos previstos en el párrafo anterior, se entenderán siempre supuestos de extrema gravedad aquellos en los que se apreciara reincidencia.

2. Cuando el hecho sea constitutivo de alguno de los delitos tipificados en los artículos 138, 139, 178, apartados 2 y 3, 179, 180, 181, apartados 2, 4, 5 y 6, y 571 a 580 del Código Penal, o de cualquier otro delito que tenga señalada en dicho Código o en las leyes penales especiales pena de prisión igual o superior a quince años, el Juez deberá imponer las medidas siguientes:

a) Si al tiempo de cometer los hechos el menor tuviere catorce o quince años de edad, una medida de internamiento en régimen cerrado de uno a cinco años de duración, complementada en su caso por otra medida de libertad vigilada de hasta tres años.

b) Si al tiempo de cometer los hechos el menor tuviere dieciséis o diecisiete años de edad, una medida de internamiento en régimen cerrado de uno a ocho años de duración, complementada en su caso por otra de libertad vigilada con asistencia educativa de hasta cinco años. En este supuesto solo podrá hacerse uso de las facultades de modificación, suspensión o sustitución de la medida impuesta a las que se refieren los artículos 13, 40 y 51.1 de esta ley orgánica, cuando haya trascurrido, al menos, la mitad de la duración de la medida de internamiento impuesta.

3. En el caso de que el delito cometido sea alguno de los comprendidos en los artículos 571 a 580 del Código Penal, el Juez, sin perjuicio de las demás medidas que correspondan con arreglo a esta Ley, también impondrá al menor una medida de inhabilitación absoluta por un tiempo superior entre cuatro y quince años al de la duración de la medida de internamiento en régimen cerrado impuesta, atendiendo proporcionalmente a la gravedad del delito, el número de los cometidos y a las circunstancias que concurran en el menor.

4. Las medidas de libertad vigilada previstas en este artículo deberán ser ratificadas mediante auto motivado, previa audiencia del Ministerio Fiscal, del letrado del menor y del representante de la entidad pública de protección o reforma de menores al finalizar el internamiento, y se llevará a cabo por las instituciones públicas encargadas del cumplimiento de las penas.

Artículo 11. *Pluralidad de infracciones.*

1. Los límites máximos establecidos en el artículo 9 y en el apartado 1 del artículo 10 serán aplicables, con arreglo a los criterios establecidos en el artículo 7, apartados 3 y 4,

aunque el menor fuere responsable de dos o más infracciones, en el caso de que éstas sean conexas o se trate de una infracción continuada, así como cuando un sólo hecho constituya dos o más infracciones. No obstante, en estos casos, el Juez, para determinar la medida o medidas a imponer, así como su duración, deberá tener en cuenta, además del interés del menor, la naturaleza y el número de las infracciones, tomando como referencia la más grave de todas ellas. Si pese a lo dispuesto en el artículo 20.1 de esta Ley dichas infracciones hubiesen sido objeto de diferentes procedimientos, el último Juez sentenciador señalará la medida o medidas que debe cumplir el menor por el conjunto de los hechos, dentro de los límites y con arreglo a los criterios expresados en el párrafo anterior.

2. Cuando alguno o algunos de los hechos a los que se refiere el apartado anterior fueren de los mencionados en el artículo 10.2 de esta Ley, la medida de internamiento en régimen cerrado podrá alcanzar una duración máxima de diez años para los mayores de dieciséis años y de seis años para los menores de esa edad, sin perjuicio de la medida de libertad vigilada que, de forma complementaria, corresponda imponer con arreglo a dicho artículo.

3. Cuando el menor hubiere cometido dos o más infracciones no comprendidas en el apartado 1 de este artículo será de aplicación lo dispuesto en el artículo 47 de la presente Ley.

Artículo 12. *Procedimiento de aplicación de medidas en supuestos de pluralidad de infracciones.*

1. A los fines previstos en el artículo anterior, en cuanto el Juez sentenciador tenga conocimiento de la existencia de otras medidas firmes en ejecución, pendientes de ejecución o suspendidas condicionalmente, impuestas al mismo menor por otros jueces de menores en anteriores sentencias, y una vez que la medida o medidas por él impuestas sean firmes, ordenará al secretario judicial que dé traslado del testimonio de su sentencia, por el medio más rápido posible, al Juez que haya dictado la primera sentencia firme, el cual será el competente para la ejecución de todas, asumiendo las funciones previstas en el apartado 2 de este artículo.

2. El Juez competente para la ejecución procederá a la refundición y a ordenar la ejecución de todas las medidas impuestas conforme establece el artículo 47 de esta Ley. Desde ese momento, pasará a ser competente a todos los efectos con exclusión de los órganos judiciales que hubieran dictado las posteriores resoluciones.

Artículo 13. *Modificación de la medida impuesta.*

1. El Juez competente para la ejecución, de oficio o a instancia del Ministerio Fiscal o del letrado del menor, previa audiencia de estos e informe del equipo técnico y, en su caso, de la entidad pública de protección o reforma de menores, podrá en cualquier momento dejar sin efecto la medida impuesta, reducir su duración o sustituirla por otra, siempre que la modificación redunde en el interés del menor y se exprese suficientemente a este el reproche merecido por su conducta. Cuando el delito cometido esté tipificado en los Capítulos I y II del Título VIII del Código Penal, sólo podrá dejarse sin efecto la medida si se acredita que la persona sometida a la misma ha cumplido la obligación prevista en el apartado 5 del artículo 7.

2. En los casos anteriores, el Juez resolverá por auto motivado, contra el cual se podrán interponer los recursos previstos en la presente Ley.

Artículo 14. *Mayoría de edad del condenado.*

1. Cuando el menor a quien se le hubiere impuesto una medida de las establecidas en esta Ley alcanzase la mayoría de edad, continuará el cumplimiento de la medida hasta alcanzar los objetivos propuestos en la sentencia en que se le impuso conforme a los criterios expresados en los artículos anteriores.

2. Cuando se trate de la medida de internamiento en régimen cerrado y el menor alcance la edad de dieciocho años sin haber finalizado su cumplimiento, el Juez de Menores, oído el Ministerio Fiscal, el letrado del menor, el equipo técnico y la entidad pública de protección o reforma de menores, podrá ordenar en auto motivado que su cumplimiento se lleve a cabo

en un centro penitenciario conforme al régimen general previsto en la Ley Orgánica General Penitenciaria si la conducta de la persona internada no responde a los objetivos propuestos en la sentencia.

3. No obstante lo señalado en los apartados anteriores, cuando las medidas de internamiento en régimen cerrado sean impuestas a quien haya cumplido veintiún años de edad o, habiendo sido impuestas con anterioridad, no hayan finalizado su cumplimiento al alcanzar la persona dicha edad, el Juez de Menores, oídos el Ministerio Fiscal, el letrado del menor, el equipo técnico y la entidad pública de protección o reforma de menores, ordenará su cumplimiento en centro penitenciario conforme al régimen general previsto en la Ley Orgánica General Penitenciaria, salvo que, excepcionalmente, entienda en consideración a las circunstancias concurrentes que procede la utilización de las medidas previstas en los artículos 13 y 51 de la presente Ley o su permanencia en el centro en cumplimiento de tal medida cuando el menor responda a los objetivos propuestos en la sentencia.

4. Cuando el menor pase a cumplir la medida de internamiento en un centro penitenciario, quedarán sin efecto el resto de medidas impuestas por el Juez de Menores que estuvieren pendientes de cumplimiento sucesivo o que estuviera cumpliendo simultáneamente con la de internamiento, si éstas no fueren compatible con el régimen penitenciario, todo ello sin perjuicio de que excepcionalmente proceda la aplicación de los artículos 13 y 51 de esta Ley.

5. La medida de internamiento en régimen cerrado que imponga el Juez de Menores con arreglo a la presente Ley se cumplirá en un centro penitenciario conforme al régimen general previsto en la Ley Orgánica General Penitenciaria siempre que, con anterioridad al inicio de la ejecución de dicha medida, el responsable hubiera cumplido ya, total o parcialmente, bien una pena de prisión impuesta con arreglo al Código Penal, o bien una medida de internamiento ejecutada en un centro penitenciario conforme a los apartados 2 y 3 de este artículo.

Artículo 15. *De la prescripción.*

1. Los hechos delictivos cometidos por los menores prescriben:

1.º Con arreglo a las normas contenidas en el Código Penal, cuando se trate de los hechos delictivos tipificados en los artículos 138, 139, 179, 180 y 571 a 580 del Código Penal o cualquier otro sancionado en el Código Penal o en las leyes penales especiales con pena de prisión igual o superior a quince años.

2.º A los cinco años, cuando se trate de un delito grave sancionado en el Código Penal con pena superior a diez años.

3.º A los tres años, cuando se trate de cualquier otro delito grave.

4.º Al año, cuando se trate de un delito menos grave. 5.º A los tres meses, cuando se trate de una falta.

2. Las medidas que tengan una duración superior a los dos años prescribirán a los tres años. Las restantes medidas prescribirán a los dos años, excepto la amonestación, las prestaciones en beneficio de la comunidad y la permanencia de fin de semana, que prescribirán al año.

[. . .]

§ 50

Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal. [Inclusión parcial]

Ministerio de Gracia y Justicia
«Gaceta de Madrid» núm. 260, de 17 de septiembre de 1882
Última modificación: 3 de enero de 2025
Referencia: BOE-A-1882-6036

Téngase en cuenta que, desde el 1 de julio de 2015, las menciones contenidas en esta ley a las "faltas" se entenderán referidas a los "delitos leves", según establece la disposición adicional 2 de la Ley Orgánica 1/2015, de 30 de marzo. Ref. BOE-A-2015-3439.
Asimismo, a partir del 1 de octubre de 2015, todas las referencias a Secretarios judiciales deberán entenderse hechas a Letrados de la Administración de Justicia, según establece la disposición adicional primera de la Ley Orgánica 7/2015, de 21 de julio. Ref. BOE-A-2015-8167
Con efectos desde el 3 de julio de 2021, las referencias contenidas en la presente Ley a la autoridad judicial o al Ministerio Fiscal, se entenderán realizadas a la Fiscalía Europea respecto de todas aquellas funciones que le atribuye el Reglamento (UE) 2017/1939 del Consejo, de 12 de octubre de 2017, según establece la disposición adicional primera de la Ley Orgánica 9/2021, de 1 de julio. Ref. BOE-A-2021-10957

Artículo 1º.

Se aprueba el adjunto proyecto de Código de Enjuiciamiento Criminal redactado con arreglo a la autorización concedida al Gobierno por la Ley sancionada en 11 de febrero de 1881 y publicada en virtud del Real Decreto de 22 de junio de 1882.

Artículo 2º.

El nuevo Código de Enjuiciamiento Criminal comenzará a regir en el tiempo y de la manera que establecen las reglas siguientes:

1.ª Se aplicará y regirá en su totalidad desde el día siguiente al en que se constituyan los Tribunales de que habla la Ley sancionada en 15 de junio de 1882 y promulgada por virtud del Real Decreto de 22 de junio del propio año.

2.ª Se aplicará y regirá desde el 15 de octubre próximo en la parte referente a la formación de los sumarios, comprendida desde el título IV del libro II hasta el art. 622 del título XI del mismo libro.

3.ª Las causas por delitos cometidos con anterioridad al 15 de octubre próximo continuarán sustanciándose con arreglo a las disposiciones del procedimiento vigente en la actualidad.

4.ª Si las causas a que se refiere la regla anterior no hubieren llegado al período de calificación, podrán sustanciarse con arreglo a las disposiciones del nuevo Código si todos los procesados en cada una de ellas optan por el nuevo procedimiento.

Para ello, el Juez que estuviere conociendo del sumario en 15 de octubre próximo hará comparecer a su presencia a todos los procesados, acompañados de sus defensores. Si aún no los tuvieren, se les nombrará de oficio para la comparecencia. Ésta se hará constar en la causa por medio de acta.

5.ª Cuando las causas por delitos cometidos con posterioridad al 15 de octubre próximo, y las que se refiere la regla anterior, alcancen el estado de conclusión del sumario antes de que se hayan constituido las nuevas Audiencias de lo criminal, se suspenderán en tal estado en los Juzgados que de ellas entiendan, debiendo remitirlas a dichas Audiencias en el mismo día en que éstas se constituyan.

6.ª Las Salas de lo Criminal de las actuales Audiencias conocerán, en tanto que se constituyan las nuevas, de los recursos que se entablen en los sumarios instruidos o continuados con sujeción a los preceptos de la nueva Ley.

Los Jueces de primera instancia se considerarán desde luego como Jueces instructores en las causas que se ajusten al nuevo procedimiento.

Artículo 3º.

Un Real Decreto fijará, con la debida anticipación, el día en que han de constituirse los nuevos Tribunales.

Artículo 4º.

Desde que cesen en sus cargos los actuales Promotores, desempeñarán las funciones del Ministerio público durante la primera instancia, en las causas que se sigan sustanciando con arreglo al procedimiento vigente en la actualidad, los Fiscales municipales que sean Letrados y, a falta de éstos, los que designen los Fiscales de las Audiencias Territoriales.

Artículo 5º.

Las Salas de Gobierno del Tribunal Supremo y de las Audiencias y, en su día, los nuevos Tribunales consultarán directamente con el Ministerio de Gracia y Justicia, para su resolución, las dudas que puedan originarse en la inteligencia y aplicación de este Real Decreto.

[. . .]

LIBRO II

Del sumario

TÍTULO I

De la denuncia

Artículo 259.

El que presenciare la perpetración de cualquier delito público está obligado a ponerlo inmediatamente en conocimiento del Juez de instrucción, de paz, comarcal o municipal o funcionario fiscal más próximo al sitio en que se hallare, bajo la multa de 25 a 250 pesetas.

Artículo 260.

La obligación establecida en el artículo anterior no comprende a los impúberes ni a los que no gozaren del pleno uso de su razón.

Artículo 261.

Tampoco estarán obligados a denunciar:

1.º Quien sea cónyuge del delincuente no separado legalmente o de hecho o la persona que conviva con él en análoga relación de afectividad.

2.º Quienes sean ascendientes y descendientes del delincuente y sus parientes colaterales hasta el segundo grado inclusive.

Esta disposición no será aplicable cuando se trate de un delito contra la vida, de un delito de homicidio, de un delito de lesiones de los artículos 149 y 150 del Código Penal, de un delito de maltrato habitual previsto en el artículo 173.2 del Código Penal, de un delito contra la libertad o contra la libertad e indemnidad sexual o de un delito de trata de seres humanos y la víctima del delito sea una persona menor de edad o una persona con discapacidad necesitada de especial protección.

Artículo 262.

Los que por razón de sus cargos, profesiones u oficios tuvieren noticia de algún delito público, estarán obligados a denunciarlo inmediatamente al Ministerio fiscal, al Tribunal competente, al Juez de instrucción y, en su defecto, al municipal o al funcionario de policía más próximo al sitio si se tratare de un delito flagrante.

Los que no cumpliesen esta obligación incurrirán en la multa señalada en el artículo 259, que se impondrá disciplinariamente.

Si la omisión en dar parte fuere de un Profesor en Medicina, Cirugía o Farmacia y tuviese relación con el ejercicio de sus actividades profesionales, la multa no podrá ser inferior a 125 pesetas ni superior a 250.

Si el que hubiese incurrido en la omisión fuere empleado público, se pondrá además en conocimiento de su superior inmediato para los efectos a que hubiere lugar en el orden administrativo.

Lo dispuesto en este artículo se entiende cuando la omisión no produjere responsabilidad con arreglo a las Leyes.

Artículo 263.

La obligación impuesta en el párrafo primero del art. anterior no comprenderá a los Abogados ni a los Procuradores respecto de las instrucciones o explicaciones que recibieren de sus clientes. Tampoco comprenderá a los eclesiásticos y ministros de cultos disidentes respecto de las noticias que se les hubieren revelado en el ejercicio de las funciones de su ministerio.

Artículo 263 bis.

1. El Juez de Instrucción competente y el Ministerio Fiscal, así como los Jefes de las Unidades Orgánicas de Policía Judicial, centrales o de ámbito provincial, y sus mandos superiores podrán autorizar la circulación o entrega vigilada de drogas tóxicas, estupefacientes o sustancias psicotrópicas, así como de otras sustancias prohibidas. Esta medida deberá acordarse por resolución fundada, en la que se determine explícitamente, en cuanto sea posible, el objeto de autorización o entrega vigilada, así como el tipo y cantidad de la sustancia de que se trate. Para adoptar estas medidas se tendrá en cuenta su necesidad a los fines de investigación en relación con la importancia del delito y con las posibilidades de vigilancia. El Juez que dicte la resolución dará traslado de copia de la misma al Juzgado Decano de su jurisdicción, el cual tendrá custodiado un registro de dichas resoluciones.

También podrá ser autorizada la circulación o entrega vigilada de los equipos, materiales y sustancias a los que se refiere el artículo 371 del Código Penal, de los bienes y ganancias a que se hace referencia en el artículo 301 de dicho Código en todos los supuestos previstos en el mismo, así como de los bienes, materiales, objetos y especies animales y vegetales a los que se refieren los artículos 332, 334, 386, 399 bis, 566, 568 y 569, también del Código Penal.

2. Se entenderá por circulación o entrega vigilada la técnica consistente en permitir que remesas ilícitas o sospechosas de drogas tóxicas, sustancias psicotrópicas u otras sustancias prohibidas, los equipos, materiales y sustancias a que se refiere el apartado anterior, las sustancias por las que se haya sustituido las anteriormente mencionadas, así como los bienes y ganancias procedentes de las actividades delictivas tipificadas en los artículos 301 a 304 y 368 a 373 del Código Penal, circulen por territorio español o salgan o

entren en él sin interferencia obstativa de la autoridad o sus agentes y bajo su vigilancia, con el fin de descubrir o identificar a las personas involucradas en la comisión de algún delito relativo a dichas drogas, sustancias, equipos, materiales, bienes y ganancias, así como también prestar auxilio a autoridades extranjeras en esos mismos fines.

3. El recurso a la entrega vigilada se hará caso por caso y, en el plano internacional, se adecuará a lo dispuesto en los tratados internacionales.

Los Jefes de las Unidades Orgánicas de la Policía Judicial centrales o de ámbito provincial o sus mandos superiores darán cuenta inmediata al Ministerio Fiscal sobre las autorizaciones que hubiesen otorgado de conformidad con el apartado 1 de este artículo y, si existiese procedimiento judicial abierto, al Juez de Instrucción competente.

4. La interceptación y apertura de envíos postales sospechosos de contener estupefacientes y, en su caso, la posterior sustitución de la droga que hubiese en su interior se llevarán a cabo respetando en todo momento las garantías judiciales establecidas en el ordenamiento jurídico, con excepción de lo previsto en el artículo 584 de la presente Ley.

Artículo 264.

El que por cualquier medio diferente de los mencionados tuviere conocimiento de la perpetración de algún delito de los que deben perseguirse de oficio, deberá denunciarlo al Ministerio Fiscal, al Tribunal competente o al Juez de instrucción o municipal, o funcionario de policía, sin que se entienda obligado por esto a probar los hechos denunciados ni a formalizar querella.

El denunciador no contraerá en ningún caso otra responsabilidad que la correspondiente a los delitos que hubiese cometido por medio de la denuncia, o con su ocasión.

Artículo 265.

1. Las denuncias podrán hacerse por escrito o de palabra, personalmente o por medio de mandatario con poder especial.

2. La denuncia contendrá la identificación de la persona denunciante y la narración circunstanciada del hecho. En caso de persona jurídica o ente sin personalidad jurídica, deberá identificarse también la persona física que formula la denuncia en su nombre, indicando su relación con la persona jurídica o el ente sin personalidad denunciante.

Igualmente, si fueran conocidas, contendrá la identificación de las personas que lo hayan cometido y de quienes lo hayan presenciado o tengan información sobre él. También indicará la existencia de cualquier fuente de conocimiento de la que el denunciante tenga noticia, que pueda servir para esclarecer el hecho denunciado.

Artículo 266.

La denuncia que se haga por escrito deberá estar firmada por el denunciante de forma autógrafa o manuscrita, si es presencial, y si no pudiere hacerlo, por otra persona a su ruego; o si se interpone por vía telemática, con firma electrónica conforme a lo establecido en artículo 10 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y en el Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE. En el caso de las personas jurídicas, se firmará con certificado electrónico cualificado con atributo de representante o los medios previstos en la regulación de firma digital que permitan identificar la persona jurídica, así como la persona física que formula la denuncia.

No se podrán denunciar por vía telemática aquellos hechos que se hayan producido con violencia o intimidación, ni si tienen autor conocido, ni si existen testigos, ni si el denunciante es menor de edad, ni si se ha cometido delito flagrante, ni aquellos hechos de naturaleza violenta o sexual.

Téngase en cuenta que esta actualización, establecida por el art. 20.2 de la Ley Orgánica 1/2025, de 2 de enero. Ref. BOE-A-2025-76, entra en vigor el 3 de abril de 2025, según determina su disposición final 38.1.

Redacción anterior:

"La denuncia que se haga por escrito deberá estar firmada por el denunciante de forma autógrafa o manuscrita, si es presencial, y si no pudiere hacerlo, por otra persona a su ruego; o si se interpone por vía telemática, con firma electrónica conforme a lo establecido en artículo 10 de la Ley 39/015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y en el Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE. En el caso de las personas jurídicas, se firmará con certificado electrónico cualificado con atributo de representante, o los medios previstos en la regulación de firma digital que permitan identificar la persona jurídica, así como la persona física que formula la denuncia."

Artículo 267.

Cuando la denuncia sea verbal, se extenderá un acta por la autoridad o funcionario que la recibiere, en la que, en forma de declaración, se expresarán cuantas noticias tenga el denunciante relativas al hecho denunciado y a sus circunstancias, firmándola ambos a continuación. Si el denunciante no pudiere firmar, lo hará otra persona a su ruego.

Artículo 268.

El Juez, Tribunal, autoridad o funcionario que recibieren una denuncia verbal o escrita harán constar por la cédula personal o por otros medios que reputen suficientes, la identidad de la persona del denunciador.

Si éste lo exigiere, le darán un resguardo de haber formalizado la denuncia.

Artículo 269.

Formalizada que sea la denuncia, se procederá o mandará proceder inmediatamente por el Juez o funcionario a quien se hiciese a la comprobación del hecho denunciado, salvo que éste no revistiere carácter de delito, o que la denuncia fuere manifiestamente falsa. En cualquiera de estos dos casos, el Tribunal o funcionario se abstendrán de todo procedimiento, sin perjuicio de la responsabilidad en que incurran si desestimasen aquélla indebidamente.

TÍTULO II

De la querella

Artículo 270.

Todos los ciudadanos españoles, hayan sido o no ofendidos por el delito, pueden querellarse, ejercitando la acción popular establecida en el artículo 101 de esta Ley.

También pueden querellarse los extranjeros por los delitos cometidos contra sus personas o bienes o las personas o bienes de sus representados, previo cumplimiento de lo dispuesto en el artículo 280, si no estuvieren comprendidos en el último párrafo del 281.

Artículo 271.

Los funcionarios del Ministerio fiscal ejercitarán también, en forma de querella, las acciones penales en los casos en que estuvieren obligados con arreglo a lo dispuesto en el artículo 105.

Artículo 272.

La querella se interpondrá ante el Juez de instrucción competente.

Si el querellado estuviere sometido por disposición especial de la Ley a determinado Tribunal, ante éste se interpondrá la querella.

Lo mismo se hará cuando fueren varios los querellados por un mismo delito o por dos o más conexos y alguno de aquéllos estuviere sometido excepcionalmente a un Tribunal que no fuere el llamado a conocer, por regla general, del delito.

Artículo 273.

En los casos del artículo anterior, cuando se trate de un delito in fraganti o de los que no dejan señales permanentes de su perpetración, o en que fuere de temer fundadamente la ocultación o fuga del presunto culpable, el particular que intentare querellarse del delito podrá acudir desde luego al Juez de instrucción o municipal que estuviere más próximo o a cualquier funcionario de policía, a fin de que se practiquen las primeras diligencias necesarias para hacer constar la verdad de los hechos y para detener al delincuente.

Artículo 274.

El particular querellante, cualquiera que sea su fuero, quedará sometido, para todos los efectos del juicio por él promovido, al Juez de instrucción o Tribunal competente para conocer del delito objeto de la querella.

Pero podrá apartarse de la querella en cualquier tiempo, quedando, sin embargo, sujeto a las responsabilidades que pudieran resultarle por sus actos anteriores.

Artículo 275.

Si la querella fuese por delito que no pueda ser perseguido sino a instancia de parte, se entenderá abandonada por el que la hubiere interpuesto cuando dejare de instar el procedimiento dentro de los diez días siguientes a la notificación del auto en que el Juez o el Tribunal así lo hubiese acordado.

Al efecto, a los diez días de haberse practicado las últimas diligencias pedidas por el querellante, o de estar paralizada la causa por falta de instancia del mismo, mandará de oficio el Juez o Tribunal que conociere de los autos que aquél pida lo que convenga a su derecho en el término fijado en el párrafo anterior.

Artículo 276.

Se tendrá también por abandonada la querella cuando, por muerte o por haberse incapacitado el querellante para continuar la acción, no compareciere ninguno de sus herederos o representantes legales a sostenerla dentro de los treinta días siguientes a la citación que al efecto se les hará dándoles conocimiento de la querella.

Artículo 277.

La querella se presentará siempre por medio de Procurador con poder bastante y suscrita por Letrado.

Se extenderá en papel de oficio, y en ella se expresará:

1.º El Juez o Tribunal ante quien se presente.

2.º El nombre, apellidos y vecindad del querellante.

3.º El nombre, apellidos y vecindad del querellado.

En el caso de ignorarse estas circunstancias, se deberá hacer la designación del querellado por las señas que mejor pudieran darle a conocer.

4.º La relación circunstanciada del hecho, con expresión del lugar, año, mes, día y hora en que se ejecutó, si se supieren.

5.º Expresión de las diligencias que se deberán practicar para la comprobación del hecho.

6.º La petición de que se admita la querella, se practiquen las diligencias indicadas en el número anterior, se proceda a la detención y prisión del presunto culpable o a exigirle la

fianza de libertad provisional, y se acuerde el embargo de sus bienes en la cantidad necesaria en los casos en que así proceda.

7.º La firma del querellante o la de otra persona a su ruego si no supiere o no pudiere firmar cuando el Procurador no tuviese poder especial para formular la querella.

Artículo 278.

Si la querella tuviere por objeto algún delito de los que solamente pueden perseguirse a instancia de parte, excepto el de violación o rapto, acompañará también la certificación que acredite haberse celebrado o intentado el acto de conciliación entre querellante y querellado.

Podrán, sin embargo, practicarse sin este requisito las diligencias de carácter urgente para la comprobación de los hechos o para la detención del delincuente, suspendiendo después el curso de los autos hasta que se acredite el cumplimiento de lo dispuesto en el párrafo anterior.

Artículo 279.

En los delitos de calumnia o injuria causadas en juicio se presentará además la licencia del Juez o Tribunal que hubiese conocido de aquél, con arreglo a lo dispuesto en el Código Penal.

Artículo 280.

El particular querellante prestará fianza de la clase y en la cuantía que fijare el Juez o Tribunal para responder de las resultas del juicio.

Artículo 281.

Quedan exentos de cumplir lo dispuesto en el artículo anterior:

1.º El ofendido y sus herederos o representantes legales.

2.º En los delitos de asesinato o de homicidio, el cónyuge del difunto o persona vinculada a él por una análoga relación de afectividad, los ascendientes y descendientes y sus parientes colaterales hasta el segundo grado inclusive, los herederos de la víctima y los padres, madres e hijos del delincuente.

3.º Las asociaciones de víctimas y las personas jurídicas a las que la ley reconoce legitimación para defender los derechos de las víctimas siempre que el ejercicio de la acción penal hubiera sido expresamente autorizado por la propia víctima.

La exención de fianza no es aplicable a los extranjeros si no les correspondiere en virtud de tratados internacionales o por el principio de reciprocidad.»

TÍTULO III

De la Policía judicial

Artículo 282.

La Policía Judicial tiene por objeto y será obligación de todos los que la componen, averiguar los delitos públicos que se cometieren en su territorio o demarcación; practicar, según sus atribuciones, las diligencias necesarias para comprobarlos y descubrir a los delincuentes, y recoger todos los efectos, instrumentos o pruebas del delito de cuya desaparición hubiere peligro, poniéndolos a disposición de la autoridad judicial. Cuando las víctimas entren en contacto con la Policía Judicial, cumplirá con los deberes de información que prevé la legislación vigente. Asimismo, llevarán a cabo una valoración de las circunstancias particulares de las víctimas para determinar provisionalmente qué medidas de protección deben ser adoptadas para garantizarles una protección adecuada, sin perjuicio de la decisión final que corresponderá adoptar al Juez o Tribunal.

Si el delito fuera de los que sólo pueden perseguirse a instancia de parte legítima, tendrán la misma obligación expresada en el párrafo anterior, si se les requiere al efecto. La

ausencia de denuncia no impedirá la práctica de las primeras diligencias de prevención y aseguramiento de los delitos relativos a la propiedad intelectual e industrial.

Artículo 282 bis.

1. A los fines previstos en el artículo anterior y cuando se trate de investigaciones que afecten a actividades propias de la delincuencia organizada, el Juez de Instrucción competente o el Ministerio Fiscal dando cuenta inmediata al Juez, podrán autorizar a funcionarios de la Policía Judicial, mediante resolución fundada y teniendo en cuenta su necesidad a los fines de la investigación, a actuar bajo identidad supuesta y a adquirir y transportar los objetos, efectos e instrumentos del delito y diferir la incautación de los mismos. La identidad supuesta será otorgada por el Ministerio del Interior por el plazo de seis meses prorrogables por períodos de igual duración, quedando legítimamente habilitados para actuar en todo lo relacionado con la investigación concreta y a participar en el tráfico jurídico y social bajo tal identidad.

La resolución por la que se acuerde deberá consignar el nombre verdadero del agente y la identidad supuesta con la que actuará en el caso concreto. La resolución será reservada y deberá conservarse fuera de las actuaciones con la debida seguridad.

La información que vaya obteniendo el agente encubierto deberá ser puesta a la mayor brevedad posible en conocimiento de quien autorizó la investigación. Asimismo, dicha información deberá aportarse al proceso en su integridad y se valorará en conciencia por el órgano judicial competente.

2. Los funcionarios de la Policía Judicial que hubieran actuado en una investigación con identidad falsa de conformidad a lo previsto en el apartado 1, podrán mantener dicha identidad cuando testifiquen en el proceso que pudiera derivarse de los hechos en que hubieran intervenido y siempre que así se acuerde mediante resolución judicial motivada, siéndole también de aplicación lo previsto en la Ley Orgánica 19/1994, de 23 de diciembre.

Ningún funcionario de la Policía Judicial podrá ser obligado a actuar como agente encubierto.

3. Cuando las actuaciones de investigación puedan afectar a los derechos fundamentales, el agente encubierto deberá solicitar del órgano judicial competente las autorizaciones que, al respecto, establezca la Constitución y la Ley, así como cumplir las demás previsiones legales aplicables.

4. A los efectos señalados en el apartado 1 de este artículo, se considerará como delincuencia organizada la asociación de tres o más personas para realizar, de forma permanente o reiterada, conductas que tengan como fin cometer alguno o algunos de los delitos siguientes:

a) Delitos de obtención, tráfico ilícito de órganos humanos y trasplante de los mismos, previstos en el artículo 156 bis del Código Penal.

b) Delito de secuestro de personas previsto en los artículos 164 a 166 del Código Penal.

c) Delito de trata de seres humanos previsto en el artículo 177 bis del Código Penal.

d) Delitos relativos a la prostitución previstos en los artículos 187 a 189 del Código Penal.

e) Delitos contra el patrimonio y contra el orden socioeconómico previstos en los artículos 237, 243, 244, 248 y 301 del Código Penal.

f) Delitos relativos a la propiedad intelectual e industrial previstos en los artículos 270 a 277 del Código Penal.

g) Delitos contra los derechos de los trabajadores previstos en los artículos 312 y 313 del Código Penal.

h) Delitos contra los derechos de los ciudadanos extranjeros previstos en el artículo 318 bis del Código Penal.

i) Delitos de tráfico de especies de flora o fauna amenazada previstos en los artículos 332 y 334 del Código Penal.

j) Delito de tráfico de material nuclear y radiactivo previsto en el artículo 345 del Código Penal.

k) Delitos contra la salud pública previstos en los artículos 368 a 373 del Código Penal.

l) Delitos de falsificación de moneda, previsto en el artículo 386 del Código Penal, y de falsificación de tarjetas de crédito o débito o cheques de viaje, previsto en el artículo 399 bis del Código Penal.

m) Delito de tráfico y depósito de armas, municiones o explosivos previsto en los artículos 566 a 568 del Código Penal.

n) Delitos de terrorismo previstos en los artículos 572 a 578 del Código Penal.

o) Delitos contra el patrimonio histórico previstos en el artículo 2.1.e de la Ley Orgánica 12/1995, de 12 de diciembre, de represión del contrabando.

5. El agente encubierto estará exento de responsabilidad criminal por aquellas actuaciones que sean consecuencia necesaria del desarrollo de la investigación, siempre que guarden la debida proporcionalidad con la finalidad de la misma y no constituyan una provocación al delito.

Para poder proceder penalmente contra el mismo por las actuaciones realizadas a los fines de la investigación, el Juez competente para conocer la causa deberá, tan pronto tenga conocimiento de la actuación de algún agente encubierto en la misma, requerir informe relativo a tal circunstancia de quien hubiere autorizado la identidad supuesta, en atención al cual resolverá lo que a su criterio proceda.

6. El juez de instrucción podrá autorizar a funcionarios de la Policía Judicial para actuar bajo identidad supuesta en comunicaciones mantenidas en canales cerrados de comunicación con el fin de esclarecer alguno de los delitos a los que se refiere el apartado 4 de este artículo o cualquier delito de los previstos en el artículo 588 ter a.

El agente encubierto informático, con autorización específica para ello, podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido y analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos.

7. En el curso de una investigación llevada a cabo mediante agente encubierto, el juez competente podrá autorizar la obtención de imágenes y la grabación de las conversaciones que puedan mantenerse en los encuentros previstos entre el agente y el investigado, aun cuando se desarrollen en el interior de un domicilio.

Artículo 283.

Constituirán la Policía judicial y serán auxiliares de los Jueces y Tribunales competentes en materia penal y del Ministerio fiscal, quedando obligados a seguir las instrucciones que de aquellas autoridades reciban a efectos de la investigación de los delitos y persecución de los delincuentes:

Primero. Las Autoridades administrativas encargadas de la seguridad pública y de la persecución de todos los delitos o de algunos especiales.

Segundo. Los empleados o subalternos de la policía de seguridad, cualquiera que sea su denominación.

Tercero. Los Alcaldes, Tenientes de Alcalde y Alcaldes de barrio.

Cuarto. Los Jefes, Oficiales e individuos de la Guardia Civil o de cualquier otra fuerza destinada a la persecución de malhechores.

Quinto. Los Serenos, Celadores y cualesquiera otros Agentes municipales de policía urbana o rural.

Sexto. Los Guardas de montes, campos y sembrados, jurados o confirmados por la Administración.

Séptimo. Los funcionarios del Cuerpo especial de Prisiones.

Octavo. Los Agentes judiciales y los subalternos de los Tribunales y Juzgados.

Noveno. El personal dependiente de la Jefatura Central de Tráfico, encargado de la investigación técnica de los accidentes.

Artículo 284.

1. Inmediatamente que los funcionarios de la Policía judicial tuvieren conocimiento de un delito público o fueren requeridos para prevenir la instrucción de diligencias por razón de algún delito privado, lo participarán a la autoridad judicial o al representante del Ministerio Fiscal, si pudieren hacerlo sin cesar en la práctica de las diligencias de prevención. En otro caso, lo harán así que las hubieren terminado.

2. No obstante, cuando no exista autor conocido del delito la Policía Judicial conservará el atestado a disposición del Ministerio Fiscal y de la autoridad judicial, sin enviárselo, salvo que concurra alguna de las siguientes circunstancias:

a) Que se trate de delitos contra la vida, contra la integridad física, contra la libertad e indemnidad sexuales o de delitos relacionados con la corrupción;
b) Que se practique cualquier diligencia después de transcurridas setenta y dos horas desde la apertura del atestado y éstas hayan tenido algún resultado; o
c) Que el Ministerio Fiscal o la autoridad judicial soliciten la remisión.

De conformidad con el derecho reconocido en el artículo 6 de la Ley 4/2015, de 27 de abril, del Estatuto de la Víctima del delito, la Policía Judicial comunicará al denunciante que en caso de no ser identificado el autor en el plazo de setenta y dos horas, las actuaciones no se remitirán a la autoridad judicial, sin perjuicio de su derecho a reiterar la denuncia ante la fiscalía o el juzgado de instrucción.
3. Si hubieran recogido armas, instrumentos o efectos de cualquier clase que pudieran tener relación con el delito y se hallen en el lugar en que éste se cometió o en sus inmediaciones, o en poder del reo o en otra parte conocida, extenderán diligencia expresiva del lugar, tiempo y ocasión en que se encontraren, que incluirá una descripción minuciosa para que se pueda formar idea cabal de los mismos y de las circunstancias de su hallazgo, que podrá ser sustituida por un reportaje gráfico. La diligencia será firmada por la persona en cuyo poder fueren hallados.
4. La incautación de efectos que pudieran pertenecer a una víctima del delito será comunicada a la misma. La persona afectada por la incautación podrá recurrir en cualquier momento la medida ante el juez de instrucción de conformidad con lo dispuesto en el párrafo tercero del artículo 334.

Artículo 285.

Si concurriere algún funcionario de Policía judicial de categoría superior a la del que estuviese actuando, deberá éste darle conocimiento de cuanto hubiese practicado, poniéndose desde luego a su disposición.

Artículo 286.

Cuando el Juez de instrucción o el municipal se presentaren a formar el sumario, cesarán las diligencias de prevención que estuviere practicando cualquier Autoridad o agente de policía; debiendo éstos entregarlas en el acto a dicho Juez, así como los efectos relativos al delito que se hubiesen recogido, y poniendo a su disposición a los detenidos, si los hubiese.

Artículo 287.

Los funcionarios que constituyen la Policía judicial practicarán sin dilación, según sus atribuciones respectivas, las diligencias que los funcionarios del Ministerio fiscal les encomienden para la comprobación del delito y averiguación de los delincuentes y todas las demás que durante el curso de la causa les encargaren los Jueces de instrucción y municipales.

Artículo 288.

El Ministerio fiscal, los Jueces de instrucción y los municipales podrán entenderse directamente con los funcionarios de Policía judicial, cualquiera que sea su categoría, para todos los efectos de este título; pero si el servicio que de ellos exigiesen admitiese espera, deberán acudir al superior respectivo del funcionario de Policía judicial, mientras no necesitasen del inmediato auxilio de éste.

Artículo 289.

El funcionario de Policía judicial que por cualquier causa no pueda cumplir el requerimiento o la orden que hubiese recibido del Ministerio fiscal, del Juez de instrucción,

del Juez municipal, o de la Autoridad o agente que hubiese prevenido las primeras diligencias, lo pondrá inmediatamente en conocimiento del que haya hecho el requerimiento o dado la orden para que provea de otro modo a su ejecución.

Artículo 290.

Si la causa no fuere legítima, el que hubiese dado la orden o hecho el requerimiento lo pondrá en conocimiento del superior jerárquico del que se excuse para que le corrija disciplinariamente, a no ser que hubiere incurrido en mayor responsabilidad con arreglo a las leyes.

El superior jerárquico comunicará a la Autoridad o funcionario que le hubiere dado la queja la resolución que adopte respecto de su subordinado.

Artículo 291.

El jefe de cualquier fuerza pública que no pudiere prestar el auxilio que por los Jueces de instrucción o municipales o por un funcionario de Policía judicial le fuere pedido se atendrá también a lo dispuesto en el artículo 289.

El que hubiere hecho el requerimiento lo pondrá en conocimiento del Jefe superior inmediato del que se excusare en la forma y para el objeto expresado en los párrafos del artículo anterior.

Artículo 292.

Los funcionarios de Policía judicial extenderán, bien en papel sellado, bien en papel común, un atestado de las diligencias que practiquen, en el cual especificarán con la mayor exactitud los hechos por ellos averiguados, insertando las declaraciones e informes recibidos y anotando todas las circunstancias que hubiesen observado y pudiesen ser prueba o indicio del delito.

La Policía Judicial remitirá con el atestado un informe dando cuenta de las detenciones anteriores y de la existencia de requisitorias para su llamamiento y busca cuando así conste en sus bases de datos.

Artículo 293.

El atestado será firmado por el que lo haya extendido, y si usare sello lo estampará con su rúbrica en todas las hojas.

Las personas presentes, peritos y testigos que hubieren intervenido en las diligencias relacionadas en el atestado serán invitadas a firmarlo en la parte a ellos referente. Si no lo hicieren, se expresará la razón.

Artículo 294.

Si no pudiere redactar el atestado el funcionario a quien correspondiese hacerlo, se sustituirá por una relación verbal circunstanciada, que reducirá a escrito de un modo fehaciente el funcionario del Ministerio fiscal, el Juez de instrucción o el municipal a quien deba presentarse el atestado, manifestándose el motivo de no haberse redactado en la forma ordinaria.

Artículo 295.

En ningún caso los funcionarios de Policía Judicial podrán dejar transcurrir más de veinticuatro horas sin dar conocimiento a la autoridad judicial o al Ministerio Fiscal de las diligencias que hubieran practicado, salvo en los supuestos de fuerza mayor y en el previsto en el apartado 2 del artículo 284.

Los que infrinjan esta disposición serán corregidos disciplinariamente con multa de 250 a 1.000 pesetas, si la omisión no mereciere la calificación de delito, y al propio tiempo será considerada dicha infracción como falta grave la primera vez y como falta muy grave las siguientes.

Los que, sin exceder el tiempo de las veinticuatro horas, demorasen más de lo necesario el dar conocimiento, serán corregidos disciplinariamente con una multa de 100 a 350

pesetas, y además esta infracción constituirá a efectos del expediente personal del interesado, falta leve la primera vez, grave las dos siguientes y muy grave las restantes.

Artículo 296.

Cuando hubieren practicado diligencias por orden o requerimiento de la Autoridad judicial o del Ministerio fiscal, comunicarán el resultado obtenido en los plazos que en la orden o en el requerimiento se hubiesen fijado.

Artículo 297.

Los atestados que redactaren y las manifestaciones que hicieren los funcionarios de Policía judicial, a consecuencia de las averiguaciones que hubiesen practicado, se considerarán denuncias para los efectos legales.

Las demás declaraciones que prestaren deberán ser firmadas, y tendrán el valor de declaraciones testificales en cuanto se refieran a hechos de conocimiento propio.

En todo caso, los funcionarios de Policía judicial están obligados a observar estrictamente las formalidades legales en cuantas diligencias practiquen, y se abstendrán bajo su responsabilidad de usar medios de averiguación que la Ley no autorice.

Artículo 298.

Los Jueces de instrucción y los Fiscales calificarán en un registro reservado el comportamiento de los funcionarios que bajo su inspección prestan servicios de Policía judicial; y cada semestre, con referencia a dicho registro, comunicarán a los superiores de cada uno de aquéllos, para los efectos a que hubiere lugar, la calificación razonada de su comportamiento.

Cuando los funcionarios de Policía judicial que hubieren de ser corregidos disciplinariamente con arreglo a esta Ley fuesen de categoría superior a la de la Autoridad judicial o fiscal que entendiesen en las diligencias en que se hubiere cometido la falta, se abstendrán éstos de imponer por sí mismos la corrección, limitándose a poner lo ocurrido en conocimiento del jefe inmediato del que debiere ser corregido.

[. . .]

TÍTULO V

De la comprobación del delito y averiguación del delincuente

[. . .]

CAPÍTULO II

Del cuerpo del delito

Artículo 334.

El Juez instructor ordenará recoger en los primeros momentos las armas, instrumentos o efectos de cualquiera clase que puedan tener relación con el delito y se hallen en el lugar en que éste se cometió, o en sus inmediaciones, o en poder del reo, o en otra parte conocida. El Secretario judicial extenderá diligencia expresiva del lugar, tiempo y ocasión en que se encontraren, describiéndolos minuciosamente para que se pueda formar idea cabal de los mismos y de las circunstancias de su hallazgo.

La diligencia será firmada por la persona en cuyo poder fueren hallados, notificándose a la misma el auto en que se mande recogerlos.

La persona afectada por la incautación podrá recurrir en cualquier momento la medida ante el Juez de Instrucción. Este recurso no requerirá de la intervención de abogado cuando sea presentado por terceras personas diferentes del imputado. El recurso se entenderá interpuesto cuando la persona afectada por la medida o un familiar suyo mayor de edad hubieran expresado su disconformidad en el momento de la misma.

Los efectos que pertenecieran a la víctima del delito serán restituidos inmediatamente a la misma, salvo que excepcionalmente debieran ser conservados como medio de prueba o para la práctica de otras diligencias, y sin perjuicio de su restitución tan pronto resulte posible. Los efectos serán también restituidos inmediatamente cuando deban ser conservados como medio de prueba o para la práctica de otras diligencias, pero su conservación pueda garantizarse imponiendo al propietario el deber de mantenerlos a disposición del Juez o Tribunal. La víctima podrá, en todo caso, recurrir esta decisión conforme a lo dispuesto en el párrafo anterior.

Artículo 335.

Siendo habida la persona o cosa objeto del delito, el Juez instructor describirá detalladamente su estado y circunstancias, y especialmente todas las que tuviesen relación con el hecho punible.

Si por tratarse de delito de falsificación cometida en documentos o efectos existentes en dependencias de las Administraciones Públicas hubiere imprescindible necesidad de tenerlos a la vista para su reconocimiento pericial y examen por parte del Juez o Tribunal, el Secretario judicial los reclamará a las correspondientes Autoridades, sin perjuicio de devolverlos a los respectivos Centros oficiales después de terminada la causa.

Artículo 336.

En los casos de los dos artículos anteriores ordenará también el Juez el reconocimiento por peritos, siempre que esté indicado para apreciar mejor la relación con el delito, de los lugares, armas, instrumentos y efectos a que dichos artículos se refieren, haciéndose constar por diligencia el reconocimiento y el informe pericial.

A esta diligencia podrán asistir también el procesado y su defensor en los términos expresados en el artículo 333.

Artículo 337.

Cuando en el acto de describir la persona o cosa objeto del delito y los lugares, armas, instrumentos o efectos relacionados con el mismo, estuvieren presentes o fueren conocidas personas que puedan declarar acerca del modo y forma con que aquél hubiese sido cometido, y de las causas de las alteraciones que se observaren en dichos lugares, armas, instrumentos o efectos, o acerca de su estado anterior, serán examinadas inmediatamente después de la descripción, y sus declaraciones se considerarán como complemento de ésta.

Artículo 338.

Sin perjuicio de lo establecido en el Capítulo II bis del presente título, los instrumentos, armas y efectos a que se refiere el artículo 334 se recogerán de tal forma que se garantice su integridad y el Juez acordará su retención, conservación o envío al organismo adecuado para su depósito.

Artículo 339.

Si fuere conveniente recibir algún informe pericial sobre los medios empleados para la desaparición del cuerpo del delito, o sobre las pruebas de cualquiera clase que en su defecto se hubiesen recogido, el Juez lo ordenará inmediatamente del modo prevenido en el capítulo VII de este mismo título.

[. . .]

Artículo 364.

En los delitos de robo, hurto, estafa y en cualquiera otro en que deba hacerse constar la preexistencia de las cosas robadas, hurtadas o estafadas, si no hubiere testigos presenciales del hecho, se recibirá información sobre los antecedentes del que se presentare como agraviado, y sobre todas las circunstancias que ofrecieren indicios de hallarse éste poseyendo aquéllas al tiempo en que resulte cometido el delito.

Artículo 365.

Cuando para la calificación del delito o de sus circunstancias fuere necesario estimar el valor de la cosa que hubiere sido su objeto o el importe del perjuicio causado o que hubiera podido causarse, el Juez oirá sobre ello al dueño o perjudicado, y acordará después el reconocimiento pericial en la forma determinada en el capítulo VII de este mismo título. El Secretario judicial facilitará a los peritos nombrados las cosas y elementos directos de apreciación sobre que hubiere de recaer el informe. Si tales efectos no estuvieren a disposición del órgano judicial, el Secretario judicial les suministrará los datos oportunos que se pudieren reunir, a fin de que, en tal caso, hagan la tasación y regulación de perjuicios de un modo prudente, con arreglo a los datos suministrados.

La valoración de las mercancías sustraídas en establecimientos comerciales se fijará atendiendo a su precio de venta al público.

Artículo 366.

Las diligencias prevenidas en este capítulo y en el anterior se practicarán con preferencia a las demás del sumario, no suspendiéndose su ejecución sino para asegurar la persona del presunto culpable o para dar el auxilio necesario a los agraviados por el delito.

Artículo 367.

En ningún caso admitirá el Juez durante el sumario reclamaciones ni tercerías que tengan por objeto la devolución de los efectos que constituyen el cuerpo del delito, cualquiera que sea su clase y la persona que los reclame.

CAPÍTULO II BIS

De la destrucción y la realización anticipada de los efectos judiciales

Artículo 367 bis.

Tendrán la consideración de efectos judiciales, en el orden penal, todos aquellos bienes puestos a disposición judicial, embargados, incautados o aprehendidos en el curso de un procedimiento penal.

Artículo 367 ter.

1. Podrá decretarse la destrucción de los efectos judiciales, dejando muestras suficientes, cuando resultare necesaria o conveniente por la propia naturaleza de los efectos intervenidos o por el peligro real o potencial que comporte su almacenamiento o custodia, previa audiencia al Ministerio Fiscal y al propietario, si fuere conocido, o a la persona en cuyo poder fueron hallados los efectos cuya destrucción se pretende.

Cuando se trate de drogas tóxicas, estupefacientes o sustancias psicotrópicas, la autoridad administrativa bajo cuya custodia se encuentren, una vez realizados los informes analíticos pertinentes, asegurada la conservación de las muestras mínimas e imprescindibles que, conforme a criterios científicos, resulten necesarias para garantizar ulteriores comprobaciones o investigaciones, y previa comunicación al Juez instructor, procederá a su inmediata destrucción si, trascurrido el plazo de un mes desde que se efectuó aquella, la autoridad judicial no hubiera ordenado mediante resolución motivada la conservación íntegra de dichas sustancias. En todo caso, lo conservado se custodiará siempre a disposición del órgano judicial competente.

2. En todo caso, el Secretario judicial extenderá la oportuna diligencia y, si se hubiera acordado la destrucción, deberá quedar constancia en los autos de la naturaleza, calidad, cantidad, peso y medida de los efectos destruidos. Si no hubiese tasación anterior, también se dejará constancia de su valor cuando su fijación fuere imposible después de la destrucción.

3. Lo dispuesto en los dos apartados anteriores será también aplicable a los efectos intervenidos en relación con la comisión de delitos contra la propiedad intelectual e industrial.

Podrá igualmente procederse a su destrucción anticipada una vez que tales efectos hayan sido examinados pericialmente, asegurando la conservación de las muestras que resulten necesarias para garantizar ulteriores comprobaciones o investigaciones, salvo que la autoridad judicial acuerde mediante resolución motivada su conservación íntegra en el plazo de un mes desde la solicitud de destrucción.

4. Si los objetos no pudieren, por su naturaleza, conservarse en su forma primitiva, el Juez resolverá lo que estime conveniente para conservarlos del mejor modo posible.

Artículo 367 quáter.

1. Podrán realizarse los efectos judiciales de lícito comercio, sin esperar al pronunciamiento o firmeza del fallo, y siempre que no se trate de piezas de convicción o que deban quedar a expensas del procedimiento, en cualquiera de los casos siguientes:

a) Cuando sean perecederos.
b) Cuando su propietario haga expreso abandono de ellos.
c) Cuando los gastos de conservación y depósito sean superiores al valor del objeto en sí.
d) Cuando su conservación pueda resultar peligrosa para la salud o seguridad pública, o pueda dar lugar a una disminución importante de su valor, o pueda afectar gravemente a su uso y funcionamiento habituales.
e) Cuando se trate de efectos que, sin sufrir deterioro material, se deprecien sustancialmente por el transcurso del tiempo.
f) Cuando, debidamente requerido el propietario sobre el destino del efecto judicial, no haga manifestación alguna.

2. Cuando concurra alguno de los supuestos previstos en el apartado anterior, el juez, de oficio o a instancia del Ministerio Fiscal, de las partes o de la Oficina de Recuperación y Gestión de Activos, y previa audiencia del interesado, acordará la realización de los efectos judiciales, salvo que concurra alguna de las siguientes circunstancias:

a) Esté pendiente de resolución el recurso interpuesto por el interesado contra el embargo o decomiso de los bienes o efectos.
b) La medida pueda resultar desproporcionada, a la vista de los efectos que pudiera suponer para el interesado y, especialmente, de la mayor o menor relevancia de los indicios en que se hubiera fundado la resolución cautelar de decomiso.

3. No obstante lo dispuesto en los apartados anteriores, cuando el bien de que se trate esté embargado en ejecución de un acuerdo adoptado por una autoridad judicial extranjera en aplicación de la Ley de reconocimiento mutuo de resoluciones penales en la Unión Europea, su realización no podrá llevarse a cabo sin obtener previamente la autorización de la autoridad judicial extranjera.

Artículo 367 quinquies.

1. La realización de los efectos judiciales podrá consistir en:

a) La entrega a entidades sin ánimo de lucro o a las Administraciones públicas.
b) La realización por medio de persona o entidad especializada.
c) La subasta pública.

2. Podrá entregarse el efecto judicial a entidades sin ánimo de lucro o a las Administraciones públicas cuando sea de ínfimo valor o se prevea que la realización por medio de persona o entidad especializada o por medio de subasta pública será antieconómica.

3. La realización de los efectos judiciales se llevará a cabo conforme al procedimiento que se determine reglamentariamente. No obstante lo anterior, previamente a acordarla se concederá audiencia al Ministerio Fiscal y a los interesados.

El producto de la realización de los efectos, bienes, instrumentos y ganancias se aplicará a los gastos que se hubieran causado en la conservación de los bienes y en el procedimiento de realización de los mismos, y la parte sobrante se ingresará en la cuenta de consignaciones del juzgado o tribunal, quedando afecta al pago de las responsabilidades

civiles y costas que se declaren, en su caso, en el procedimiento. También podrá asignarse total o parcialmente de manera definitiva, en los términos y por el procedimiento que reglamentariamente se establezcan, a la Oficina de Recuperación y Gestión de Activos y a los órganos del Ministerio Fiscal encargados de la represión de las actividades de las organizaciones criminales. Todo ello sin perjuicio de lo dispuesto para el Fondo de bienes decomisados por tráfico ilícito de drogas y otros delitos relacionados.

En el caso de realización de un bien embargado o decomisado por orden de una autoridad judicial extranjera se aplicará lo dispuesto en la Ley de reconocimiento mutuo de resoluciones penales en la Unión Europea.

Artículo 367 sexies.

1. Podrá autorizarse la utilización provisional de los bienes o efectos decomisados cautelarmente en los siguientes casos:

a) Cuando concurran las circunstancias expresadas en las letras b) a f) del apartado 1 del artículo 367 quater, y la utilización de los efectos permita a la Administración un aprovechamiento de su valor mayor que con la realización anticipada, o no se considere procedente la realización anticipada de los mismos.

b) Cuando se trate de efectos especialmente idóneos para la prestación de un servicio público.

2. Cuando concurra alguno de los supuestos previstos en el apartado anterior, el juez, de oficio o a instancia del Ministerio Fiscal o de la Oficina de Recuperación y Gestión de activos, y previa audiencia del interesado, autorizará la utilización provisional de los efectos judiciales, salvo que concurra alguna de las circunstancias expresadas en el párrafo segundo del apartado 2 del artículo 367 quater.

3. Corresponderá a la Oficina de Recuperación y Gestión de activos resolver, conforme a lo previsto legal y reglamentariamente, sobre la adjudicación del uso de los efectos decomisados cautelarmente y sobre las medidas de conservación que deban ser adoptadas. La oficina informará al juez o tribunal, y al Fiscal, de lo que hubiera acordado.

Artículo 367 septies.

El juez o tribunal, de oficio o a instancia del Ministerio Fiscal o de la propia Oficina de Recuperación y Gestión de activos, podrá encomendar la localización, la conservación y la administración de los efectos, bienes, instrumentos y ganancias procedentes de actividades delictivas cometidas en el marco de una organización criminal a la Oficina de Recuperación y Gestión de Activos.

La organización y funcionamiento de dicha Oficina se regularán reglamentariamente.

CAPÍTULO III

De la identidad del delincuente y de sus circunstancias personales

Artículo 368.

Cuantos dirijan cargo a determinada persona deberán reconocerla judicialmente, si el Juez instructor, los acusadores o el mismo inculpado conceptúan fundadamente precisa la diligencia para la identificación de este último, con relación a los designantes, a fin de que no ofrezca duda quién es la persona a que aquéllos se refieren.

Artículo 369.

La diligencia de reconocimiento se practicará poniendo a la vista del que hubiere de verificarlo la persona que haya de ser reconocida, haciéndola comparecer en unión con otras de circunstancias exteriores semejantes. A presencia de todas ellas, o desde un punto en que no pudiere ser visto, según al Juez pareciere más conveniente, el que deba practicar el reconocimiento manifestará si se encuentra en la rueda o grupo la persona a quien hubiese hecho referencia en sus declaraciones, designándola, en caso afirmativo, clara y determinadamente.

En la diligencia que se extienda se harán constar todas las circunstancias del acto, así como los nombres de todos los que hubiesen formado la rueda o grupo.

Artículo 370.

Cuando fueren varios los que hubieren de reconocer a una persona, la diligencia expresada en el artículo anterior deberá practicarse separadamente con cada uno de ellos, sin que puedan comunicarse entre sí hasta que se haya efectuado el último reconocimiento.

Cuando fueren varios los que hubieren de ser reconocidos por una misma persona, podrá hacerse el reconocimiento de todos en un solo acto.

Artículo 371.

El que detuviere o prendiere a algún presunto culpable tomará las precauciones necesarias para que el detenido o preso no haga en su persona o traje alteración alguna que pueda dificultar su reconocimiento por quien corresponda.

Artículo 372.

Análogas precauciones deberán tomar los Alcaides de las cárceles y los Jefes de los depósitos de detenidos; y si en los establecimientos de su cargo hubiere traje reglamentario, conservarán cuidadosamente el que lleven los presos o detenidos al ingresar en el establecimiento, a fin de que puedan vestirlo cuantas veces fuere conveniente para diligencias de reconocimiento.

Artículo 373.

Si se originase alguna duda sobre la identidad del procesado, se procurará acreditar ésta por cuantos medios fueren conducentes al objeto.

Artículo 374.

El Juez hará constar, con la minuciosidad posible, las señas personales del procesado, a fin de que la diligencia pueda servir de prueba de su identidad.

Artículo 375.

Para acreditar la edad del procesado y comprobar la identidad de su persona, el Secretario judicial traerá al sumario certificación de su inscripción de nacimiento en el Registro civil o de su partida de bautismo, si no estuviere inscrito en el Registro.

En todo caso, cuando no fuere posible averiguar el Registro civil o parroquia en que deba constar el nacimiento o el bautismo del procesado, o no existiesen su inscripción y partida; y cuando por manifestar el procesado haber nacido en punto lejano hubiere necesidad de emplear mucho tiempo en traer a la causa la certificación oportuna, no se detendrá el sumario, y se suplirá el documento del artículo anterior por informes que acerca de la edad del procesado, y previo su examen físico, dieren los Médicos forenses o los nombrados por el Juez.

Artículo 376.

Cuando no ofreciere duda la identidad del procesado, y conocidamente tuviese la edad que el Código penal requiere para poderle exigir la responsabilidad criminal en toda su extensión, podrá prescindirse de la justificación expresada en el artículo anterior, si su práctica ofreciese alguna dificultad u ocasionase dilaciones extraordinarias.

En las actuaciones sucesivas y durante el juicio, el procesado será designado con el nombre con que fuere conocido o con el que él mismo dijere tener.

Artículo 377.

Si el Juez instructor lo considerase conveniente, podrá pedir informes sobre el procesado a las Alcaldías o a los correspondientes funcionarios de policía del pueblo o pueblos en que hubiese residido.

Estos informes serán fundados, y si no fuere posible fundarlos, se manifestará la causa que lo impidiere.

Los que los dieren no contraerán responsabilidad alguna, salvo en el caso de dolo o negligencia grave.

Artículo 378.

Podrá además el Juez recibir declaración acerca de la conducta del procesado a todas las personas que por el conocimiento que tuvieren de éste puedan ilustrarle sobre ello.

Artículo 379.

Se traerán a la causa los antecedentes penales del procesado, pidiendo los anteriores a la creación del Registro Central de Penados de 2 de octubre de 1878, a los Juzgados donde se presuma que puedan en su caso constar, y los posteriores exclusivamente al Ministerio de Gracia y Justicia.

El Jefe del Registro en el Ministerio está obligado a dar los antecedentes que se le reclamen, o certificación negativa, en su caso, en el improrrogable término de tres días, a contar desde aquel en que se reciba la petición, justificando, si así no lo hiciere, la causa legítima que lo hubiese impedido.

En los Juzgados se atenderá también preferentemente al cumplimiento de este servicio, debiendo ser corregidos disciplinariamente los funcionarios que lo posterguen.

Artículo 380.

Si el procesado fuere mayor de nueve años y menor de quince, el Juez recibirá información acerca del criterio del mismo, y especialmente de su aptitud para apreciar la criminalidad del hecho que hubiese dado motivo a la causa.

En esta información serán oídas las personas que puedan deponer con acierto por sus circunstancias personales y por las relaciones que hayan tenido con el procesado antes y después de haberse ejecutado el hecho. En su defecto se nombrarán dos Profesores de instrucción primaria para que, en unión del Médico forense o del que haga sus veces, examinen al procesado y emitan su dictamen.

Artículo 381.

Si el Juez advirtiese en el procesado indicios de enajenación mental, le someterá inmediatamente a la observación de los Médicos forenses en el establecimiento en que estuviese preso, o en otro público si fuere más a propósito o estuviese en libertad.

Los Médicos darán en tal caso su informe del modo expresado en el capítulo VII de este título.

Artículo 382.

Sin perjuicio de lo dispuesto en el artículo anterior, el Juez recibirá información acerca de la enajenación mental del procesado, en la forma prevenida en el artículo 380.

Artículo 383.

Si la demencia sobreviniera después de cometido el delito, concluso que sea el sumario se mandará archivar la causa por el Tribunal competente hasta que el procesado recobre la salud, disponiéndose además respecto de éste lo que el Código Penal prescribe para los que ejecutan el hecho en estado de demencia.

Si hubiese algún otro procesado por razón del mismo delito que no se encontrase en el caso del anterior, continuará la causa solamente en cuanto al mismo.

Artículo 384.

Desde que resultare del sumario algún indicio racional de criminalidad contra determinada persona, se dictará auto declarándola procesada y mandando que se entiendan

con ella las diligencias en la forma y del modo dispuesto en este título y en los demás de esta Ley.

El procesado podrá, desde el momento de serlo, aconsejarse de Letrado, mientras no estuviere incomunicado, y valerse de él, bien para instar la pronta terminación del sumario, bien para solicitar la práctica de diligencias que le interesen, y para formular pretensiones que afecten a su situación. En el primer caso podrán recurrir en queja a la Audiencia, y en los otros dos apelar para ante la misma si el Juez instructor no accediese a sus deseos.

Estas apelaciones no serán admisibles más que en un solo efecto.

Para cumplir lo determinado en este artículo, el Juez instructor dispondrá que el procesado menor de edad sea habilitado de Procurador y Abogado, a no ser que él mismo o su representante legal designen personas que merezcan su confianza para dicha representación y defensa.

Contra los autos que dicten los Jueces de instrucción, decretando el procesamiento de alguna persona, podrá utilizarse, por la representación de ésta, recurso de reforma dentro de los tres días siguientes al de haberle sido notificada la resolución; y contra los autos denegatorios de la reforma podrá ser interpuesto recurso de apelación en un efecto dentro de los cinco días siguientes al de la notificación del auto denegatorio a la representación recurrente. También podrá ser interpuesto el recurso de apelación en un efecto subsidiariamente con el de reforma, en cuyo caso, el Juez instructor declarará admitido aquél al denegar éste. Si se diera lugar a la reforma, quedando sin efecto los procesamientos antes acordados, se estará a lo preceptuado en el párrafo siguiente, en cuanto a la reproducción de la solicitud de procesamiento ante la Audiencia.

Contra los autos denegatorios de procesamiento, sólo se concederá a quien haya solicitado éstos el recurso de reforma, utilizándolo dentro de los tres días siguientes al de la notificación. Contra los autos denegatorios de la reforma así pretendida, no se podrá utilizar recurso de apelación ni ningún otro recurso; pero podrá reproducirse ante la Audiencia correspondiente la petición de procesamiento formulada por la parte a quien le haya sido denegada, cuando, personada ante dicho Tribunal, si hace uso de tal derecho, evacue el traslado a que se refiere el artículo 627 de esta misma Ley, precisamente dentro del término por el cual le haya sido conferido dicho traslado. El Tribunal, en tales casos, al dictar el auto que ordena el artículo 630, resolverá fundadamente lo que proceda; y sin que pueda dejar al criterio del instructor la resolución, cuando estime procedentes las declaraciones de procesamiento solicitadas, mandará al Juez instructor que las haga. Los procesados a quienes estas resoluciones del instructor se refieran podrán utilizar directamente el recurso de apelación en un efecto, sin necesidad de que utilicen previamente el de reforma.

Cuando la resolución del recurso de reforma interpuesto contra un auto denegatorio de procesamiento sea favorable al recurrente y, por tanto, se acuerde el procesamiento primeramente solicitado contra la resolución en que así se declara, podrán las representaciones de los procesados a quienes afecte utilizar los mismos recursos de reforma y apelación otorgados a los procesados directamente en este mismo artículo.

Artículo 384 bis.

Firme un auto de procesamiento y decretada la prisión provisional por delito cometido por persona integrada o relacionada con bandas armadas o individuos terroristas o rebeldes, el procesado que estuviere ostentando función o cargo público quedará automáticamente suspendido en el ejercicio del mismo mientras dure la situación de prisión.

[. . .]

CAPÍTULO VII

Del informe pericial

Artículo 456.

El Juez acordará el informe pericial cuando, para conocer o apreciar algún hecho o circunstancia importante en el sumario, fuesen necesarios o convenientes conocimientos científicos o artísticos.

Artículo 457.

Los peritos pueden ser o no titulares.

Son peritos titulares los que tienen título oficial de una ciencia o arte cuyo ejercicio esté reglamentado por la Administración.

Son peritos no titulares los que, careciendo de título oficial, tienen, sin embargo, conocimiento o prácticas especiales en alguna ciencia o arte.

Artículo 458.

El Juez se valdrá de peritos titulares con preferencia a los que no tuviesen título.

Artículo 459.

Todo reconocimiento pericial se hará por dos peritos.

Se exceptúa el caso en que no hubiese más de uno en el lugar y no fuere posible esperar la llegada de otro sin graves inconvenientes para el curso del sumario.

Artículo 460.

El nombramiento se hará saber a los peritos por medio de oficio, que les será entregado por alguacil o portero del Juzgado, con las formalidades prevenidas para la citación de los testigos, reemplazándose la cédula original, para los efectos del artículo 175, por un atestado que extenderá el alguacil o portero encargado de la entrega.

Artículo 461.

Si la urgencia del caso lo exige, podrá hacerse el llamamiento verbalmente de orden del Juez, haciéndolo constar así en los autos; pero extendiendo siempre el atestado prevenido en el artículo anterior el encargado del cumplimiento de la orden de llamamiento.

Artículo 462.

Nadie podrá negarse a acudir al llamamiento del Juez para desempeñar un servicio pericial, si no estuviese legítimamente impedido.

En este caso deberá ponerlo en conocimiento del Juez en el acto de recibir el nombramiento, para que se provea a lo que haya lugar.

Artículo 463.

El perito que sin alegar excusa fundada deje de acudir al llamamiento del Juez o se niegue a prestar el informe, incurrirá en las responsabilidades señaladas para los testigos en el artículo 420.

Artículo 464.

No podrán prestar informe pericial acerca del delito, cualquiera que sea la persona ofendida, los que según el artículo 416 no están obligados a declarar como testigos.

El perito que, hallándose comprendido en alguno de los casos de dicho artículo, preste el informe sin poner antes esa circunstancia en conocimiento del Juez que le hubiese nombrado incurrirá en la multa de 200 a 5.000 euros, a no ser que el hecho diere lugar a responsabilidad criminal.

Artículo 465.

Los que presten informe como peritos en virtud de orden judicial tendrán derecho a reclamar los honorarios e indemnizaciones que sean justas, si no tuvieren, en concepto de tales peritos, retribución fija satisfecha por el Estado, por la Provincia o por el Municipio.

Artículo 466.

Hecho el nombramiento de peritos, el Secretario judicial lo notificará inmediatamente al Ministerio Fiscal, al actor particular, si lo hubiere, como al procesado, si estuviere a

disposición del Juez o se encontrare en el mismo lugar de la instrucción, o a su representante si lo tuviere.

Artículo 467.

Si el reconocimiento e informe periciales pudieren tener lugar de nuevo en el juicio oral, los peritos nombrados no podrán ser recusados por las partes.

Si no pudiere reproducirse en el juicio oral, habrá lugar a la recusación.

Artículo 468.

Son causa de recusación de los peritos:

1.º El parentesco de consanguinidad o de afinidad dentro del cuarto grado con el querellante o con el reo.

2.º El interés directo o indirecto en la causa o en otra semejante.

3.º La amistad íntima o la enemistad manifiesta.

Artículo 469.

El actor o el procesado que intente recusar al perito o peritos nombrados por el Juez deberá hacerlo por escrito antes de empezar la diligencia pericial, expresando la causa de la recusación y la prueba testifical que ofrezca, y acompañando la documental o designando el lugar en que ésta se halle si no la tuviere a su disposición.

Para la presentación de este escrito no estará obligado a valerse de Procurador.

Artículo 470.

El Juez, sin levantar mano, examinará los documentos que produzca el recusante y oirá a los testigos que presente en el acto, resolviendo lo que estime justo respecto de la recusación.

Si hubiere lugar a ella, suspenderá el acto pericial por el tiempo estrictamente necesario para nombrar el perito que haya de sustituir al recusado, hacérselo saber y constituirse el nombrado en el lugar correspondiente.

Si no la admitiere, se procederá como si no se hubiese usado de la facultad de recusar.

Cuando el recusante no produjese los documentos, pero designare el archivo o lugar en que se encuentren, se reclamarán por el Secretario judicial, y el Juez instructor los examinará una vez recibidos sin detener por esto el curso de las actuaciones; y si de ellos resultase justificada la causa de la recusación, anulará el informe pericial que se hubiese dado, mandando que se practique de nuevo esta diligencia.

Artículo 471.

En el caso del párrafo segundo del artículo 467, el querellante tendrá derecho a nombrar a su costa un perito que intervenga en el acto pericial.

El mismo derecho tendrá el procesado.

Si los querellantes o los procesados fuesen varios, se pondrán, respectivamente, de acuerdo entre sí para hacer el nombramiento.

Estos peritos deberán ser titulares, a no ser que no los hubiere de esta clase en el partido o demarcación, en cuyo caso podrán ser nombrados sin título.

Si la práctica de la diligencia pericial no admitiere espera, se procederá como las circunstancias lo permitan para que el actor y el procesado puedan intervenir en ella.

Artículo 472.

Si las partes hicieren uso de la facultad que se les concede en el artículo anterior, manifestarán al Juez el nombre del perito y ofrecerán al hacer esta manifestación los comprobantes de tener la cualidad de tal perito la persona designada.

En ningún caso podrán hacer uso de dicha facultad después de empezada la operación de reconocimiento.

Artículo 473.

El Juez resolverá sobre la admisión de dichos peritos en la forma determinada en el artículo 470 para las recusaciones.

Artículo 474.

Antes de darse principio al acto pericial, todos los peritos, así los nombrados por el Juez como los que lo hubieren sido por las partes, prestarán juramento, conforme al artículo 434, de proceder bien y fielmente en sus operaciones y de no proponerse otro fin más que el de descubrir y declarar la verdad.

Artículo 475.

El Juez manifestará clara y determinadamente a los peritos el objeto de su informe.

Artículo 476.

Al acto pericial podrán concurrir, en el caso del párrafo segundo del artículo 467, el querellante, si lo hubiere, con su representación, y el procesado con la suya, aun cuando estuviere preso, en cuyo caso adoptará el Juez las precauciones oportunas.

Artículo 477.

El acto pericial será presidido por el Juez instructor o, en virtud de su delegación, por el Juez municipal. Podrá también delegar, en el caso del artículo 353, en un funcionario de Policía judicial.

Asistirá siempre el Secretario que actúe en la causa.

Artículo 478.

El informe pericial comprenderá, si fuere posible:

1.º Descripción de la persona o cosa que sea objeto del mismo en el estado o del modo en que se halle.

El Secretario extenderá esta descripción, dictándola los peritos y suscribiéndola todos los concurrentes.

2.º Relación detallada de todas las operaciones practicadas por los peritos y de su resultado, extendida y autorizada en la misma forma que la anterior.

3.º Las conclusiones que en vista de tales datos formulen los peritos conforme a los principios y reglas de su ciencia o arte.

Artículo 479.

Si los peritos tuvieren necesidad de destruir o alterar los objetos que analicen, deberá conservarse, a ser posible, parte de ellos a disposición del Juez, para que, en caso necesario, pueda hacerse nuevo análisis.

Artículo 480.

Las partes que asistieren a las operaciones o reconocimientos podrán someter a los peritos las observaciones que estimen convenientes, haciéndose constar todas en la diligencia.

Artículo 481.

Hecho el reconocimiento, podrán los peritos, si lo pidieran, retirarse por el tiempo absolutamente preciso al sitio que el Juez les señale para deliberar y redactar las conclusiones.

Artículo 482.

Si los peritos necesitaren descanso, el Juez o el funcionario que le represente podrá concederles para ello el tiempo necesario.

También podrá suspender la diligencia hasta otra hora u otro día, cuando lo exigiere su naturaleza.

En este caso, el Juez o quien lo represente adoptará las precauciones convenientes para evitar cualquier alteración en la materia de la diligencia pericial.

Artículo 483.

El Juez podrá, por su propia iniciativa o por reclamación de las partes presentes o de sus defensores, hacer a los peritos, cuando produzcan sus conclusiones, las preguntas que estime pertinentes y pedirles las aclaraciones necesarias.

Las contestaciones de los peritos se considerarán como parte de su informe.

Artículo 484.

Si los peritos estuviesen discordes y su número fuere par, nombrará otro el Juez.

Con intervención del nuevamente nombrado, se repetirán, si fuere posible, las operaciones que hubiesen practicado aquéllos, y se ejecutarán las demás que parecieren oportunas.

Si no fuere posible la repetición de las operaciones ni la práctica de otras nuevas, la intervención del perito últimamente nombrado se limitará a deliberar con los demás, con vista de las diligencias de reconocimiento practicadas, y a formular luego con quien estuviere conforme, o separadamente si no lo estuviese con ninguno, sus conclusiones motivadas.

Artículo 485.

El Juez facilitará a los peritos los medios materiales necesarios para practicar la diligencia que les encomiende, reclamándolos de la Administración pública, o dirigiendo a la autoridad correspondiente un aviso previo si existieren preparados para tal objeto, salvo lo dispuesto especialmente en el artículo 362.

[. . .]

TÍTULO VIII

De las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución

CAPÍTULO I

De la entrada y registro en lugar cerrado

Artículo 545.

Nadie podrá entrar en el domicilio de un español o extranjero residente en España sin su consentimiento, excepto en los casos y en la forma expresamente previstos en las leyes.

Artículo 546.

El Juez o Tribunal que conociere de la causa podrá decretar la entrada y registro, de día o de noche, en todos los edificios y lugares públicos, sea cualquiera el territorio en que radiquen, cuando hubiere indicios de encontrarse allí el procesado o efectos o instrumentos del delito, o libros, papeles u otros objetos que puedan servir para su descubrimiento y comprobación.

Artículo 547.

Se reputarán edificios o lugares públicos para la observancia de lo dispuesto en este capítulo:

1.º Los que estuvieren destinados a cualquier servicio oficial, militar o civil del Estado, de la Provincia o del Municipio, aunque habiten allí los encargados de dicho servicio o los de la conservación y custodia del edificio o lugar.

2.º Los que estuvieren destinados a cualquier establecimiento de reunión o recreo, fueren o no lícitos.

3.º Cualesquiera otros edificios o lugares cerrados que no constituyeren domicilio de un particular con arreglo a lo dispuesto en el artículo 554.

4.º Los buques del Estado.

Artículo 548.

El Juez necesitará para la entrada y registro en el Palacio de cualquiera de los Cuerpos Colegisladores la autorización del Presidente respectivo.

Artículo 549.

Para la entrada y registro en los templos y demás lugares religiosos bastará pasar recado de atención a las personas a cuyo cargo estuvieren.

Artículo 550.

Podrá asimismo el Juez instructor ordenar en los casos indicados en el artículo 546 la entrada y registro, de día o de noche, si la urgencia lo hiciere necesario, en cualquier edificio o lugar cerrado o parte de él, que constituya domicilio de cualquier español o extranjero residente en España, pero precediendo siempre el consentimiento del interesado conforme se previene en el artículo 6.º de la Constitución, o a falta de consentimiento, en virtud de auto motivado, que se notificará a la persona interesada inmediatamente, o lo más tarde dentro de las veinticuatro horas de haberse dictado.

Artículo 551.

Se entenderá que presta su consentimiento aquel que, requerido por quien hubiere de efectuar la entrada y registro para que los permita, ejecuta por su parte los actos necesarios que de él dependan para que puedan tener efecto, sin invocar la inviolabilidad que reconoce al domicilio el artículo 6.º de la Constitución del Estado[(*)].

[(*)]Actualmente art. 18.2 de la Constitución Española.

Artículo 552.

Al practicar los registros deberán evitarse las inspecciones inútiles, procurando no perjudicar ni importunar al interesado más de lo necesario, y se adoptarán todo género de precauciones para no comprometer su reputación, respetando sus secretos si no interesaren a la instrucción.

Artículo 553.

Los Agentes de policía podrán asimismo proceder de propia autoridad a la inmediata detención de las personas cuando haya mandamiento de prisión contra ellas, cuando sean sorprendidas en flagrante delito, cuando un delincuente, inmediatamente perseguido por los Agentes de la autoridad, se oculte o refugie en alguna casa o, en casos de excepcional o urgente necesidad, cuando se trate de presuntos responsables de las acciones a que se refiere el artículo 384 bis, cualquiera que fuese el lugar o domicilio donde se ocultasen o refugiasen, así como al registro que, con ocasión de aquélla, se efectúe en dichos lugares y a la ocupación de los efectos e instrumentos que en ellos se hallasen y que pudieran guardar relación con el delito perseguido.

Del registro efectuado, conforme a lo establecido en el párrafo anterior, se dará cuenta inmediata al Juez competente, con indicación de las causas que lo motivaron y de los resultados obtenidos en el mismo, con especial referencia a las detenciones que, en su caso, se hubieran practicado. Asimismo, se indicarán las personas que hayan intervenido y los incidentes ocurridos.

Artículo 554.

Se reputan domicilio, para los efectos de los artículos anteriores:

1.º Los Palacios Reales, estén o no habitados por el Monarca al tiempo de la entrada o registro.

2.º El edificio o lugar cerrado, o la parte de él destinada principalmente a la habitación de cualquier español o extranjero residente en España y de su familia.

3.º Los buques nacionales mercantes.

4.º Tratándose de personas jurídicas imputadas, el espacio físico que constituya el centro de dirección de las mismas, ya se trate de su domicilio social o de un establecimiento dependiente, o aquellos otros lugares en que se custodien documentos u otros soportes de su vida diaria que quedan reservados al conocimiento de terceros.

Artículo 555.

Para registrar en el Palacio en que se halle residiendo el Monarca, solicitará el Juez real licencia por conducto del Mayordomo Mayor de Su Majestad.

Artículo 556.

En los Sitios Reales en que no se hallare el Monarca al tiempo del registro, será necesaria la licencia del Jefe o empleado del servicio de Su Majestad que tuviera a su cargo la custodia del edificio, o la del que haga sus veces cuando se solicitare, si estuviere ausente.

Artículo 557.

(Anulado)

Artículo 558.

El auto de entrada y registro en el domicilio de un particular será siempre fundado, y el Juez expresará en él concretamente el edificio o lugar cerrado en que haya de verificarse, si tendrá lugar tan sólo de día y la Autoridad o funcionario que los haya de practicar.

Artículo 559.

Para la entrada y registro en los edificios destinados a la habitación u oficina de los representantes de naciones extranjeras acreditados cerca del Gobierno de España, les pedirá su venia el Juez, por medio de atento oficio, en el que les rogará que contesten en el término de doce horas.

Artículo 560.

Si transcurriese este término sin haberlo hecho, o si el representante extranjero denegare la venia, el Juez lo comunicará inmediatamente al Ministerio de Gracia y Justicia, empleando para ello el telégrafo, si lo hubiere. Entre tanto que el Ministro no le comunique su resolución, se abstendrá de entrar y registrar en el edificio; pero adoptará las medidas de vigilancia a que se refiere el artículo 567.

Artículo 561.

En los buques extranjeros de guerra, la falta de autorización del Comandante se suplirá por la del Embajador o Ministro de la nación a que pertenezcan.

Artículo 562.

Se podrá entrar en las habitaciones de los Cónsules extranjeros y en sus oficinas pasándoles previamente recado de atención y observando las formalidades prescritas en la Constitución del Estado y en las leyes.

Artículo 563.

Si el edificio o lugar cerrado estuviese en el territorio propio del Juez instructor, podrá encomendar la entrada y registro al Juez municipal del territorio en que el edificio o lugar cerrado radiquen, o a cualquier Autoridad o agente de Policía judicial. Si el que lo hubiese ordenado fuere el Juez municipal, podrá encomendarlo también a dichas Autoridades o agentes de Policía judicial.

Cuando el edificio o lugar cerrado estuviere fuera del territorio del Juez, encomendará éste la práctica de las operaciones al Juez de su propia categoría del territorio en que aquéllos radiquen, el cual, a su vez, podrá encomendarlas a las Autoridades o agentes de Policía judicial.

Artículo 564.

Si se tratare de un edificio o lugar público comprendido en los números 1.º y 3.º del artículo 547, el Juez oficiará a la Autoridad o Jefe de que aquéllos dependan en la misma población.

Si éste no contestare en el término que se le fije en el oficio, se notificará el auto en que se disponga la entrada y registro al encargado de la conservación o custodia del edificio o lugar en que se hubiere de entrar y registrar.

Si se tratare de buques del Estado, las comunicaciones se dirigirán a los Comandantes respectivos.

Artículo 565.

Cuando el edificio o lugar fueren de los comprendidos en el número 2.º del artículo 547, la notificación se hará a la persona que se halle al frente del establecimiento de reunión o recreo, o a quien haga sus veces si aquél estuviere ausente.

Artículo 566.

Si la entrada y registro se hubieren de hacer en el domicilio de un particular, se notificará el auto a éste; y si no fuere habido a la primera diligencia en busca, a su encargado.

Si no fuere tampoco habido el encargado, se hará la notificación a cualquier otra persona mayor de edad que se hallare en el domicilio, prefiriendo para esto a los individuos de la familia del interesado.

Si no se halla a nadie, se hará constar por diligencia, que se extenderá con asistencia de dos vecinos, los cuales deberán firmarla.

Artículo 567.

Desde el momento en que el Juez acuerde la entrada y registro en cualquier edificio o lugar cerrado, adoptará las medidas de vigilancia convenientes para evitar la fuga del procesado o la sustracción de los instrumentos, efectos del delito, libros, papeles o cualesquiera otras cosas que hayan de ser objeto del registro.

Artículo 568.

Practicadas las diligencias que se establecen en los artículos anteriores, se procederá a la entrada y registro, empleando para ello, si fuere necesario, el auxilio de la fuerza.

Artículo 569.

El registro se hará a presencia del interesado o de la persona que legítimamente le represente.

Si aquél no fuere habido o no quisiese concurrir ni nombrar representante, se practicará a presencia de un individuo de su familia mayor de edad.

Si no le hubiere, se hará a presencia de dos testigos, vecinos del mismo pueblo.

El registro se practicará siempre en presencia del Secretario del Juzgado o Tribunal que lo hubiera autorizado, o del Secretario del servicio de guardia que le sustituya, quien levantará acta del resultado, de la diligencia y de sus incidencias y que será firmada por

todos los asistentes. No obstante, en caso de necesidad, el Secretario judicial podrá ser sustituido en la forma prevista en la Ley Orgánica del Poder Judicial.

La resistencia del interesado, de su representante, de los individuos de la familia y de los testigos a presenciar el registro producirá la responsabilidad declarada en el Código Penal a los reos del delito de desobediencia grave a la Autoridad, sin perjuicio de que la diligencia se practique.

Si no se encontrasen las personas u objetos que se busquen ni apareciesen indicios sospechosos, se expedirá una certificación del acta a la parte interesada si la reclamare.

Artículo 570.

Cuando el registro se practique en el domicilio de un particular y expire el día sin haberse terminado, el que lo haga requerirá al interesado o a su representante, si estuviere presente, para que permita la continuación durante la noche. Si se opusiere, se suspenderá la diligencia, salvo lo dispuesto en los artículos 546 y 550, cerrando y sellando el local o los muebles en que hubiere de continuarse, en cuanto esta precaución se considere necesaria para evitar la fuga de la persona o la sustracción de las cosas que se buscaren.

Prevendrá asimismo el que practique el registro a los que se hallen en el edificio o lugar de la diligencia que no levanten los sellos, ni violenten las cerraduras, ni permitan que lo hagan otras personas, bajo la responsabilidad establecida en el Código Penal.

Artículo 571.

El registro no se suspenderá sino por el tiempo en que no fuere posible continuarle, y se adoptarán, durante la suspensión, las medidas de vigilancia a que se refiere el artículo 567.

Artículo 572.

En la diligencia de entrada y registro en lugar cerrado, se expresarán los nombres del Juez, o de su delegado, que la practique y de las demás personas que intervengan, los incidentes ocurridos, la hora en que se hubiese principiado y concluido la diligencia, y la relación del registro por el orden con que se haga, así como los resultados obtenidos.

CAPÍTULO II

Del registro de libros y papeles

Artículo 573.

No se ordenará el registro de los libros y papeles de contabilidad del procesado o de otra persona sino cuando hubiere indicios graves de que de esta diligencia resultará el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa.

Artículo 574.

El Juez ordenará recoger los instrumentos y efectos del delito y también los libros, papeles o cualesquiera otras cosas que se hubiesen encontrado, si esto fuere necesario para el resultado del sumario.

Los libros y papeles que se recojan serán foliados, sellados y rubricados en todas sus hojas por el Secretario judicial, bajo su responsabilidad.

Artículo 575.

Todos están obligados a exhibir los objetos y papeles que se sospeche puedan tener relación con la causa.

Si el que los retenga se negare a su exhibición, será corregido con multa de 125 a 500 pesetas; y cuando insistiera en su negativa, si el objeto o papel fueren de importancia y la índole del delito lo aconseje, será procesado como autor del de desobediencia a la Autoridad, salvo si mereciera la calificación legal de encubridor o receptador.

Artículo 576.

Será aplicable al registro de papeles y efectos lo establecido en los artículos 552 y 569.

Artículo 577.

Si para determinar sobre la necesidad de recoger las cosas que se hubiesen encontrado en el registro fuere necesario algún reconocimiento pericial, se acordará en el acto por el Juez, en la forma establecida en el capítulo VII del título V.

Artículo 578.

Si el libro que haya de ser objeto del registro fuere el protocolo de un Notario, se procederá con arreglo a lo dispuesto en la Ley del Notariado.

Si se tratare de un libro del Registro de la Propiedad, se estará a lo ordenado en la Ley Hipotecaria.

Si se tratare de un libro del Registro Civil o Mercantil se estará a lo que se disponga en la Ley y Reglamentos relativos a estos servicios.

CAPÍTULO III

De la detención y apertura de la correspondencia escrita y telegráfica

Artículo 579. *De la correspondencia escrita o telegráfica.*

1. El juez podrá acordar la detención de la correspondencia privada, postal y telegráfica, incluidos faxes, burofaxes y giros, que el investigado remita o reciba, así como su apertura o examen, si hubiera indicios de obtener por estos medios el descubrimiento o la comprobación del algún hecho o circunstancia relevante para la causa, siempre que la investigación tenga por objeto alguno de los siguientes delitos:

1.º Delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión.

2.º Delitos cometidos en el seno de un grupo u organización criminal.

3.º Delitos de terrorismo.

2. El juez podrá acordar, en resolución motivada, por un plazo de hasta tres meses, prorrogable por iguales o inferiores períodos hasta un máximo de dieciocho meses, la observación de las comunicaciones postales y telegráficas del investigado, así como de las comunicaciones de las que se sirva para la realización de sus fines delictivos.

3. En caso de urgencia, cuando las investigaciones se realicen para la averiguación de delitos relacionados con la actuación de bandas armadas o elementos terroristas y existan razones fundadas que hagan imprescindible la medida prevista en los apartados anteriores de este artículo, podrá ordenarla el Ministro del Interior o, en su defecto, el Secretario de Estado de Seguridad. Esta medida se comunicará inmediatamente al juez competente y, en todo caso, dentro del plazo máximo de veinticuatro horas, haciendo constar las razones que justificaron la adopción de la medida, la actuación realizada, la forma en que se ha efectuado y su resultado. El juez competente, también de forma motivada, revocará o confirmará tal actuación en un plazo máximo de setenta y dos horas desde que fue ordenada la medida.

4. No se requerirá autorización judicial en los siguientes casos:

a) Envíos postales que, por sus propias características externas, no sean usualmente utilizados para contener correspondencia individual sino para servir al transporte y tráfico de mercancías o en cuyo exterior se haga constar su contenido.

b) Aquellas otras formas de envío de la correspondencia bajo el formato legal de comunicación abierta, en las que resulte obligatoria una declaración externa de contenido o que incorporen la indicación expresa de que se autoriza su inspección.

c) Cuando la inspección se lleve a cabo de acuerdo con la normativa aduanera o proceda con arreglo a las normas postales que regulan una determinada clase de envío.

5. La solicitud y las actuaciones posteriores relativas a la medida solicitada se sustanciarán en una pieza separada y secreta, sin necesidad de que se acuerde expresamente el secreto de la causa.

Artículo 579 bis. *Utilización de la información obtenida en un procedimiento distinto y descubrimientos casuales.*

1. El resultado de la detención y apertura de la correspondencia escrita y telegráfica podrá ser utilizado como medio de investigación o prueba en otro proceso penal.
2. A tal efecto, se procederá a la deducción de testimonio de los particulares necesarios para acreditar la legitimidad de la injerencia. Se incluirán entre los antecedentes indispensables, en todo caso, la solicitud inicial para la adopción, la resolución judicial que la acuerda y todas las peticiones y resoluciones judiciales de prórroga recaídas en el procedimiento de origen.
3. La continuación de esta medida para la investigación del delito casualmente descubierto requiere autorización del juez competente, para la cual, éste comprobará la diligencia de la actuación, evaluando el marco en el que se produjo el hallazgo casual y la imposibilidad de haber solicitado la medida que lo incluyera en su momento. Asimismo se informará si las diligencias continúan declaradas secretas, a los efectos de que tal declaración sea respetada en el otro proceso penal, comunicando el momento en el que dicho secreto se alce.

Artículo 580.

Es aplicable a la detención de la correspondencia lo dispuesto en los artículos 563 y 564.
Podrá también encomendarse la práctica de esta operación al Administrador de Correos y Telégrafos o Jefe de la oficina en que la correspondencia deba hallarse.

Artículo 581.

El empleado que haga la detención remitirá inmediatamente la correspondencia detenida al Juez instructor de la causa.

Artículo 582.

Podrá asimismo el Juez ordenar que por cualquier Administración de Telégrafos se le faciliten copias de los telegramas por ella transmitidos, si pudieran contribuir al esclarecimiento de los hechos de la causa.

Artículo 583.

El auto motivado acordando la detención y registro de la correspondencia o la entrega de copias de telegramas transmitidos determinará la correspondencia que haya de ser detenida o registrada, o los telegramas cuyas copias hayan de ser entregadas, por medio de la designación de las personas a cuyo nombre se hubieran expedido, o por otras circunstancias igualmente concretas.

Artículo 584.

Para la apertura y registro de la correspondencia postal será citado el interesado.
Éste o la persona que designe podrá presenciar la operación.

Artículo 585.

Si el procesado estuviere en rebeldía, o si citado para la apertura no quisiere presenciarla ni nombrar persona para que lo haga en su nombre, el Juez instructor procederá, sin embargo, a la apertura de dicha correspondencia.

Artículo 586.

La operación se practicará abriendo el Juez por sí mismo la correspondencia, y después de leerla para sí apartará la que haga referencia a los hechos de la causa y cuya conservación considere necesaria.

Los sobres y hojas de esta correspondencia, después de haber tomado el mismo Juez las notas necesarias para la práctica de otras diligencias de investigación a que la correspondencia diere motivo, se rubricarán por el Secretario judicial y se sellarán con el sello del Juzgado, encerrándolo todo después en otro sobre, al que se pondrá el rótulo necesario, conservándose durante el sumario, también bajo responsabilidad del Secretario judicial.

Este pliego podrá abrirse cuantas veces el Juez lo considere preciso, citando previamente al interesado.

Artículo 587.

La correspondencia que no se relacione con la causa será entregada en el acto al procesado o a su representante.

Si aquél estuviere en rebeldía, se entregará cerrada a un individuo de su familia mayor de edad.

Si no fuere conocido ningún pariente del procesado, se conservará dicho pliego cerrado bajo la responsabilidad del Secretario judicial hasta que haya persona a quien entregarlo, según lo dispuesto en este artículo.

Artículo 588.

La apertura de la correspondencia se hará constar por diligencia, en la que se referirá cuanto en aquélla hubiese ocurrido.

Esta diligencia será firmada por el Juez instructor, el Secretario y demás asistentes.

CAPÍTULO IV

Disposiciones comunes a la interceptación de las comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen, el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos

Artículo 588 bis a. *Principios rectores.*

1. Durante la instrucción de las causas se podrá acordar alguna de las medidas de investigación reguladas en el presente capítulo siempre que medie autorización judicial dictada con plena sujeción a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida.

2. El principio de especialidad exige que una medida esté relacionada con la investigación de un delito concreto. No podrán autorizarse medidas de investigación tecnológica que tengan por objeto prevenir o descubrir delitos o despejar sospechas sin base objetiva.

3. El principio de idoneidad servirá para definir el ámbito objetivo y subjetivo y la duración de la medida en virtud de su utilidad.

4. En aplicación de los principios de excepcionalidad y necesidad solo podrá acordarse la medida:

a) cuando no estén a disposición de la investigación, en atención a sus características, otras medidas menos gravosas para los derechos fundamentales del investigado o encausado e igualmente útiles para el esclarecimiento del hecho, o

b) cuando el descubrimiento o la comprobación del hecho investigado, la determinación de su autor o autores, la averiguación de su paradero, o la localización de los efectos del delito se vea gravemente dificultada sin el recurso a esta medida.

5. Las medidas de investigación reguladas en este capítulo solo se reputarán proporcionadas cuando, tomadas en consideración todas las circunstancias del caso, el sacrificio de los derechos e intereses afectados no sea superior al beneficio que de su adopción resulte para el interés público y de terceros. Para la ponderación de los intereses en conflicto, la valoración del interés público se basará en la gravedad del hecho, su trascendencia social o el ámbito tecnológico de producción, la intensidad de los indicios existentes y la relevancia del resultado perseguido con la restricción del derecho.

Artículo 588 bis b. *Solicitud de autorización judicial.*

1. El juez podrá acordar las medidas reguladas en este capítulo de oficio o a instancia del Ministerio Fiscal o de la Policía Judicial.

2. Cuando el Ministerio Fiscal o la Policía Judicial soliciten del juez de instrucción una medida de investigación tecnológica, la petición habrá de contener:

1.º La descripción del hecho objeto de investigación y la identidad del investigado o de cualquier otro afectado por la medida, siempre que tales datos resulten conocidos.

2.º La exposición detallada de las razones que justifiquen la necesidad de la medida de acuerdo a los principios rectores establecidos en el artículo 588 bis a, así como los indicios de criminalidad que se hayan puesto de manifiesto durante la investigación previa a la solicitud de autorización del acto de injerencia.

3.º Los datos de identificación del investigado o encausado y, en su caso, de los medios de comunicación empleados que permitan la ejecución de la medida.

4.º La extensión de la medida con especificación de su contenido.

5.º La unidad investigadora de la Policía Judicial que se hará cargo de la intervención.

6.º La forma de ejecución de la medida.

7.º La duración de la medida que se solicita.

8.º El sujeto obligado que llevará a cabo la medida, en caso de conocerse.

Artículo 588 bis c. *Resolución judicial.*

1. El juez de instrucción autorizará o denegará la medida solicitada mediante auto motivado, oído el Ministerio Fiscal. Esta resolución se dictará en el plazo máximo de veinticuatro horas desde que se presente la solicitud.

2. Siempre que resulte necesario para resolver sobre el cumplimiento de alguno de los requisitos expresados en los artículos anteriores, el juez podrá requerir, con interrupción del plazo a que se refiere el apartado anterior, una ampliación o aclaración de los términos de la solicitud.

3. La resolución judicial que autorice la medida concretará al menos los siguientes extremos:

a) El hecho punible objeto de investigación y su calificación jurídica, con expresión de los indicios racionales en los que funde la medida.

b) La identidad de los investigados y de cualquier otro afectado por la medida, de ser conocido.

c) La extensión de la medida de injerencia, especificando su alcance así como la motivación relativa al cumplimiento de los principios rectores establecidos en el artículo 588 bis a.

d) La unidad investigadora de Policía Judicial que se hará cargo de la intervención.

e) La duración de la medida.

f) La forma y la periodicidad con la que el solicitante informará al juez sobre los resultados de la medida.

g) La finalidad perseguida con la medida.

h) El sujeto obligado que llevará a cabo la medida, en caso de conocerse, con expresa mención del deber de colaboración y de guardar secreto, cuando proceda, bajo apercibimiento de incurrir en un delito de desobediencia.

Artículo 588 bis d. *Secreto.*

La solicitud y las actuaciones posteriores relativas a la medida solicitada se sustanciarán en una pieza separada y secreta, sin necesidad de que se acuerde expresamente el secreto de la causa.

Artículo 588 bis e. *Duración.*

1. Las medidas reguladas en el presente capítulo tendrán la duración que se especifique para cada una de ellas y no podrán exceder del tiempo imprescindible para el esclarecimiento de los hechos.
2. La medida podrá ser prorrogada, mediante auto motivado, por el juez competente, de oficio o previa petición razonada del solicitante, siempre que subsistan las causas que la motivaron.
3. Transcurrido el plazo por el que resultó concedida la medida, sin haberse acordado su prórroga, o, en su caso, finalizada ésta, cesará a todos los efectos.

Artículo 588 bis f. *Solicitud de prórroga.*

1. La solicitud de prórroga se dirigirá por el Ministerio Fiscal o la Policía Judicial al juez competente con la antelación suficiente a la expiración del plazo concedido. Deberá incluir en todo caso:

a) Un informe detallado del resultado de la medida.
b) Las razones que justifiquen la continuación de la misma.

2. En el plazo de los dos días siguientes a la presentación de la solicitud, el juez resolverá sobre el fin de la medida o su prórroga mediante auto motivado. Antes de dictar la resolución podrá solicitar aclaraciones o mayor información.
3. Concedida la prórroga, su cómputo se iniciará desde la fecha de expiración del plazo de la medida acordada.

Artículo 588 bis g. *Control de la medida.*

La Policía Judicial informará al juez de instrucción del desarrollo y los resultados de la medida, en la forma y con la periodicidad que este determine y, en todo caso, cuando por cualquier causa se ponga fin a la misma.

Artículo 588 bis h. *Afectación de terceras personas.*

Podrán acordarse las medidas de investigación reguladas en los siguientes capítulos aun cuando afecten a terceras personas en los casos y con las condiciones que se regulan en las disposiciones específicas de cada una de ellas.

Artículo 588 bis i. *Utilización de la información obtenida en un procedimiento distinto y descubrimientos casuales.*

El uso de las informaciones obtenidas en un procedimiento distinto y los descubrimientos casuales se regularan con arreglo a lo dispuesto en el artículo 579 bis.

Artículo 588 bis j. *Cese de la medida.*

El juez acordará el cese de la medida cuando desaparezcan las circunstancias que justificaron su adopción o resulte evidente que a través de la misma no se están obteniendo los resultados pretendidos, y, en todo caso, cuando haya transcurrido el plazo para el que hubiera sido autorizada.

Artículo 588 bis k. *Destrucción de registros.*

1. Una vez que se ponga término al procedimiento mediante resolución firme, se ordenará el borrado y eliminación de los registros originales que puedan constar en los sistemas electrónicos e informáticos utilizados en la ejecución de la medida. Se conservará una copia bajo custodia del secretario judicial.

2. Se acordará la destrucción de las copias conservadas cuando hayan transcurrido cinco años desde que la pena se haya ejecutado o cuando el delito o la pena hayan prescrito o se haya decretado el sobreseimiento libre o haya recaído sentencia absolutoria firme respecto del investigado, siempre que no fuera precisa su conservación a juicio del Tribunal.

3. Los tribunales dictarán las órdenes oportunas a la Policía Judicial para que lleve a efecto la destrucción contemplada en los anteriores apartados.

CAPÍTULO V

La interceptación de las comunicaciones telefónicas y telemáticas

Sección 1.ª Disposiciones generales

Artículo 588 ter a. *Presupuestos.*

La autorización para la interceptación de las comunicaciones telefónicas y telemáticas solo podrá ser concedida cuando la investigación tenga por objeto alguno de los delitos a que se refiere el artículo 579.1 de esta ley o delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación.

Artículo 588 ter b. *Ámbito.*

1. Los terminales o medios de comunicación objeto de intervención han de ser aquellos habitual u ocasionalmente utilizados por el investigado.

2. La intervención judicialmente acordada podrá autorizar el acceso al contenido de las comunicaciones y a los datos electrónicos de tráfico o asociados al proceso de comunicación, así como a los que se produzcan con independencia del establecimiento o no de una concreta comunicación, en los que participe el sujeto investigado, ya sea como emisor o como receptor, y podrá afectar a los terminales o los medios de comunicación de los que el investigado sea titular o usuario.

También podrán intervenirse los terminales o medios de comunicación de la víctima cuando sea previsible un grave riesgo para su vida o integridad.

A los efectos previstos en este artículo, se entenderá por datos electrónicos de tráfico o asociados todos aquellos que se generan como consecuencia de la conducción de la comunicación a través de una red de comunicaciones electrónicas, de su puesta a disposición del usuario, así como de la prestación de un servicio de la sociedad de la información o comunicación telemática de naturaleza análoga.

Artículo 588 ter c. *Afectación a tercero.*

Podrá acordarse la intervención judicial de las comunicaciones emitidas desde terminales o medios de comunicación telemática pertenecientes a una tercera persona siempre que:

1.º exista constancia de que el sujeto investigado se sirve de aquella para transmitir o recibir información, o

2.º el titular colabore con la persona investigada en sus fines ilícitos o se beneficie de su actividad.

También podrá autorizarse dicha intervención cuando el dispositivo objeto de investigación sea utilizado maliciosamente por terceros por vía telemática, sin conocimiento de su titular.

Artículo 588 ter d. *Solicitud de autorización judicial.*

1. La solicitud de autorización judicial deberá contener, además de los requisitos mencionados en el artículo 588 bis b, los siguientes:

a) la identificación del número de abonado, del terminal o de la etiqueta técnica,

b) la identificación de la conexión objeto de la intervención o

c) los datos necesarios para identificar el medio de telecomunicación de que se trate.

2. Para determinar la extensión de la medida, la solicitud de autorización judicial podrá tener por objeto alguno de los siguientes extremos:

a) El registro y la grabación del contenido de la comunicación, con indicación de la forma o tipo de comunicaciones a las que afecta.
b) El conocimiento de su origen o destino, en el momento en el que la comunicación se realiza.
c) La localización geográfica del origen o destino de la comunicación.
d) El conocimiento de otros datos de tráfico asociados o no asociados pero de valor añadido a la comunicación. En este caso, la solicitud especificará los datos concretos que han de ser obtenidos.

3. En caso de urgencia, cuando las investigaciones se realicen para la averiguación de delitos relacionados con la actuación de bandas armadas o elementos terroristas y existan razones fundadas que hagan imprescindible la medida prevista en los apartados anteriores de este artículo, podrá ordenarla el Ministro del Interior o, en su defecto, el Secretario de Estado de Seguridad. Esta medida se comunicará inmediatamente al juez competente y, en todo caso, dentro del plazo máximo de veinticuatro horas, haciendo constar las razones que justificaron la adopción de la medida, la actuación realizada, la forma en que se ha efectuado y su resultado. El juez competente, también de forma motivada, revocará o confirmará tal actuación en un plazo máximo de setenta y dos horas desde que fue ordenada la medida.

Artículo 588 ter e. *Deber de colaboración.*

1. Todos los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, así como toda persona que de cualquier modo contribuya a facilitar las comunicaciones a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual, están obligados a prestar al juez, al Ministerio Fiscal y a los agentes de la Policía Judicial designados para la práctica de la medida la asistencia y colaboración precisas para facilitar el cumplimiento de los autos de intervención de las telecomunicaciones.
2. Los sujetos requeridos para prestar colaboración tendrán la obligación de guardar secreto acerca de las actividades requeridas por las autoridades.
3. Los sujetos obligados que incumplieren los anteriores deberes podrán incurrir en delito de desobediencia.

Artículo 588 ter f. *Control de la medida.*

En cumplimiento de lo dispuesto en el artículo 588 bis g, la Policía Judicial pondrá a disposición del juez, con la periodicidad que este determine y en soportes digitales distintos, la transcripción de los pasajes que considere de interés y las grabaciones íntegras realizadas. Se indicará el origen y destino de cada una de ellas y se asegurará, mediante un sistema de sellado o firma electrónica avanzado o sistema de adveración suficientemente fiable, la autenticidad e integridad de la información volcada desde el ordenador central a los soportes digitales en que las comunicaciones hubieran sido grabadas.

Artículo 588 ter g. *Duración.*

La duración máxima inicial de la intervención, que se computará desde la fecha de autorización judicial, será de tres meses, prorrogables por períodos sucesivos de igual duración hasta el plazo máximo de dieciocho meses.

Artículo 588 ter h. *Solicitud de prórroga.*

Para la fundamentación de la solicitud de la prórroga, la Policía Judicial aportará, en su caso, la transcripción de aquellos pasajes de las conversaciones de las que se deduzcan informaciones relevantes para decidir sobre el mantenimiento de la medida.
Antes de dictar la resolución, el juez podrá solicitar aclaraciones o mayor información, incluido el contenido íntegro de las conversaciones intervenidas.

Artículo 588 ter i. *Acceso de las partes a las grabaciones.*

1. Alzado el secreto y expirada la vigencia de la medida de intervención, se entregará a las partes copia de las grabaciones y de las transcripciones realizadas. Si en la grabación hubiera datos referidos a aspectos de la vida íntima de las personas, solo se entregará la grabación y transcripción de aquellas partes que no se refieran a ellos. La no inclusión de la totalidad de la grabación en la transcripción entregada se hará constar de modo expreso.

2. Una vez examinadas las grabaciones y en el plazo fijado por el juez, en atención al volumen de la información contenida en los soportes, cualquiera de las partes podrá solicitar la inclusión en las copias de aquellas comunicaciones que entienda relevantes y hayan sido excluidas. El juez de instrucción, oídas o examinadas por sí esas comunicaciones, decidirá sobre su exclusión o incorporación a la causa.

3. Se notificará por el juez de instrucción a las personas intervinientes en las comunicaciones interceptadas el hecho de la práctica de la injerencia y se les informará de las concretas comunicaciones en las que haya participado que resulten afectadas, salvo que sea imposible, exija un esfuerzo desproporcionado o puedan perjudicar futuras investigaciones. Si la persona notificada lo solicita se le entregará copia de la grabación o transcripción de tales comunicaciones, en la medida que esto no afecte al derecho a la intimidad de otras personas o resulte contrario a los fines del proceso en cuyo marco se hubiere adoptado la medida de injerencia.

Sección 2.ª Incorporación al proceso de datos electrónicos de tráfico o asociados

Artículo 588 ter j. *Datos obrantes en archivos automatizados de los prestadores de servicios.*

1. Los datos electrónicos conservados por los prestadores de servicios o personas que faciliten la comunicación en cumplimiento de la legislación sobre retención de datos relativos a las comunicaciones electrónicas o por propia iniciativa por motivos comerciales o de otra índole y que se encuentren vinculados a procesos de comunicación, solo podrán ser cedidos para su incorporación al proceso con autorización judicial.

2. Cuando el conocimiento de esos datos resulte indispensable para la investigación, se solicitará del juez competente autorización para recabar la información que conste en los archivos automatizados de los prestadores de servicios, incluida la búsqueda entrecruzada o inteligente de datos, siempre que se precisen la naturaleza de los datos que hayan de ser conocidos y las razones que justifican la cesión.

Sección 3.ª Acceso a los datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad

Artículo 588 ter k. *Identificación mediante número IP.*

Cuando en el ejercicio de las funciones de prevención y descubrimiento de los delitos cometidos en internet, los agentes de la Policía Judicial tuvieran acceso a una dirección IP que estuviera siendo utilizada para la comisión algún delito y no constara la identificación y localización del equipo o del dispositivo de conectividad correspondiente ni los datos de identificación personal del usuario, solicitarán del juez de instrucción que requiera de los agentes sujetos al deber de colaboración según el artículo 588 ter e, la cesión de los datos que permitan la identificación y localización del terminal o del dispositivo de conectividad y la identificación del sospechoso.

Artículo 588 ter l. *Identificación de los terminales mediante captación de códigos de identificación del aparato o de sus componentes.*

1. Siempre que en el marco de una investigación no hubiera sido posible obtener un determinado número de abonado y este resulte indispensable a los fines de la investigación, los agentes de Policía Judicial podrán valerse de artificios técnicos que permitan acceder al conocimiento de los códigos de identificación o etiquetas técnicas del aparato de telecomunicación o de alguno de sus componentes, tales como la numeración IMSI o IMEI y,

en general, de cualquier medio técnico que, de acuerdo con el estado de la tecnología, sea apto para identificar el equipo de comunicación utilizado o la tarjeta utilizada para acceder a la red de telecomunicaciones.

2. Una vez obtenidos los códigos que permiten la identificación del aparato o de alguno de sus componentes, los agentes de la Policía Judicial podrán solicitar del juez competente la intervención de las comunicaciones en los términos establecidos en el artículo 588 ter d. La solicitud habrá de poner en conocimiento del órgano jurisdiccional la utilización de los artificios a que se refiere el apartado anterior.

El tribunal dictará resolución motivada concediendo o denegando la solicitud de intervención en el plazo establecido en el artículo 588 bis c.

Artículo 588 ter m. *Identificación de titulares o terminales o dispositivos de conectividad.*

Cuando, en el ejercicio de sus funciones, el Ministerio Fiscal o la Policía Judicial necesiten conocer la titularidad de un número de teléfono o de cualquier otro medio de comunicación, o, en sentido inverso, precisen el número de teléfono o los datos identificativos de cualquier medio de comunicación, podrán dirigirse directamente a los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, quienes estarán obligados a cumplir el requerimiento, bajo apercibimiento de incurrir en el delito de desobediencia.

CAPÍTULO VI

Captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos

Artículo 588 quater a. *Grabación de las comunicaciones orales directas.*

1. Podrá autorizarse la colocación y utilización de dispositivos electrónicos que permitan la captación y grabación de las comunicaciones orales directas que se mantengan por el investigado, en la vía pública o en otro espacio abierto, en su domicilio o en cualesquiera otros lugares cerrados.

Los dispositivos de escucha y grabación podrán ser colocados tanto en el exterior como en el interior del domicilio o lugar cerrado.

2. En el supuesto en que fuera necesaria la entrada en el domicilio o en alguno de los espacios destinados al ejercicio de la privacidad, la resolución habilitante habrá de extender su motivación a la procedencia del acceso a dichos lugares.

3. La escucha y grabación de las conversaciones privadas se podrá complementar con la obtención de imágenes cuando expresamente lo autorice la resolución judicial que la acuerde.

Artículo 588 quater b. *Presupuestos.*

1. La utilización de los dispositivos a que se refiere el artículo anterior ha de estar vinculada a comunicaciones que puedan tener lugar en uno o varios encuentros concretos del investigado con otras personas y sobre cuya previsibilidad haya indicios puestos de manifiesto por la investigación.

2. Solo podrá autorizarse cuando concurran los requisitos siguientes:

a) Que los hechos que estén siendo investigados sean constitutivos de alguno de los siguientes delitos:

1.º Delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión.

2.º Delitos cometidos en el seno de un grupo u organización criminal.

3.º Delitos de terrorismo.

b) Que pueda racionalmente preverse que la utilización de los dispositivos aportará datos esenciales y de relevancia probatoria para el esclarecimiento de los hechos y la identificación de su autor.

Artículo 588 quater c. *Contenido de la resolución judicial.*

La resolución judicial que autorice la medida, deberá contener, además de las exigencias reguladas en el artículo 588 bis c, una mención concreta al lugar o dependencias, así como a los encuentros del investigado que van a ser sometidos a vigilancia.

Artículo 588 quater d. *Control de la medida.*

En cumplimiento de lo dispuesto en el artículo 588 bis g, la Policía Judicial pondrá a disposición de la autoridad judicial el soporte original o copia electrónica auténtica de las grabaciones e imágenes, que deberá ir acompañado de una transcripción de las conversaciones que considere de interés.

El informe identificará a todos los agentes que hayan participado en la ejecución y seguimiento de la medida.

Artículo 588 quater e. *Cese.*

Cesada la medida por alguna de las causas previstas en el artículo 588 bis j, la grabación de conversaciones que puedan tener lugar en otros encuentros o la captación de imágenes de tales momentos exigirán una nueva autorización judicial.

CAPÍTULO VII

Utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización

Artículo 588 quinquies a. *Captación de imágenes en lugares o espacios públicos.*

1. La Policía Judicial podrá obtener y grabar por cualquier medio técnico imágenes de la persona investigada cuando se encuentre en un lugar o espacio público, si ello fuera necesario para facilitar su identificación, para localizar los instrumentos o efectos del delito u obtener datos relevantes para el esclarecimiento de los hechos.

2. La medida podrá ser llevada a cabo aun cuando afecte a personas diferentes del investigado, siempre que de otro modo se reduzca de forma relevante la utilidad de la vigilancia o existan indicios fundados de la relación de dichas personas con el investigado y los hechos objeto de la investigación.

Artículo 588 quinquies b. *Utilización de dispositivos o medios técnicos de seguimiento y localización.*

1. Cuando concurran acreditadas razones de necesidad y la medida resulte proporcionada, el juez competente podrá autorizar la utilización de dispositivos o medios técnicos de seguimiento y localización.

2. La autorización deberá especificar el medio técnico que va a ser utilizado.

3. Los prestadores, agentes y personas a que se refiere el artículo 588 ter e están obligados a prestar al juez, al Ministerio Fiscal y a los agentes de la Policía Judicial designados para la práctica de la medida la asistencia y colaboración precisas para facilitar el cumplimiento de los autos por los que se ordene el seguimiento, bajo apercibimiento de incurrir en delito de desobediencia.

4. Cuando concurran razones de urgencia que hagan razonablemente temer que de no colocarse inmediatamente el dispositivo o medio técnico de seguimiento y localización se frustrará la investigación, la Policía Judicial podrá proceder a su colocación, dando cuenta a la mayor brevedad posible, y en todo caso en el plazo máximo de veinticuatro horas, a la autoridad judicial, quien podrá ratificar la medida adoptada o acordar su inmediato cese en el mismo plazo. En este último supuesto, la información obtenida a partir del dispositivo colocado carecerá de efectos en el proceso.

Artículo 588 quinquies c. *Duración de la medida.*

1. La medida de utilización de dispositivos técnicos de seguimiento y localización prevista en el artículo anterior tendrá una duración máxima de tres meses a partir de la fecha

de su autorización. Excepcionalmente, el juez podrá acordar prórrogas sucesivas por el mismo o inferior plazo hasta un máximo de dieciocho meses, si así estuviera justificado a la vista de los resultados obtenidos con la medida.

2. La Policía Judicial entregará al juez los soportes originales o copias electrónicas auténticas que contengan la información recogida cuando éste se lo solicite y, en todo caso, cuando terminen las investigaciones.

3. La información obtenida a través de los dispositivos técnicos de seguimiento y localización a los que se refieren los artículos anteriores deberá ser debidamente custodiada para evitar su utilización indebida.

CAPÍTULO VIII

Registro de dispositivos de almacenamiento masivo de información

Artículo 588 sexies a. *Necesidad de motivación individualizada.*

1. Cuando con ocasión de la práctica de un registro domiciliario sea previsible la aprehensión de ordenadores, instrumentos de comunicación telefónica o telemática o dispositivos de almacenamiento masivo de información digital o el acceso a repositorios telemáticos de datos, la resolución del juez de instrucción habrá de extender su razonamiento a la justificación, en su caso, de las razones que legitiman el acceso de los agentes facultados a la información contenida en tales dispositivos.

2. La simple incautación de cualquiera de los dispositivos a los que se refiere el apartado anterior, practicada durante el transcurso de la diligencia de registro domiciliario, no legitima el acceso a su contenido, sin perjuicio de que dicho acceso pueda ser autorizado ulteriormente por el juez competente.

Artículo 588 sexies b. *Acceso a la información de dispositivos electrónicos incautados fuera del domicilio del investigado.*

La exigencia prevista en el apartado 1 del artículo anterior será también aplicable a aquellos casos en los que los ordenadores, instrumentos de comunicación o dispositivos de almacenamiento masivo de datos, o el acceso a repositorios telemáticos de datos, sean aprehendidos con independencia de un registro domiciliario. En tales casos, los agentes pondrán en conocimiento del juez la incautación de tales efectos. Si éste considera indispensable el acceso a la información albergada en su contenido, otorgará la correspondiente autorización.

Artículo 588 sexies c. *Autorización judicial.*

1. La resolución del juez de instrucción mediante la que se autorice el acceso a la información contenida en los dispositivos a que se refiere la presente sección, fijará los términos y el alcance del registro y podrá autorizar la realización de copias de los datos informáticos. Fijará también las condiciones necesarias para asegurar la integridad de los datos y las garantías de su preservación para hacer posible, en su caso, la práctica de un dictamen pericial.

2. Salvo que constituyan el objeto o instrumento del delito o existan otras razones que lo justifiquen, se evitará la incautación de los soportes físicos que contengan los datos o archivos informáticos, cuando ello pueda causar un grave perjuicio a su titular o propietario y sea posible la obtención de una copia de ellos en condiciones que garanticen la autenticidad e integridad de los datos.

3. Cuando quienes lleven a cabo el registro o tengan acceso al sistema de información o a una parte del mismo conforme a lo dispuesto en este capítulo, tengan razones fundadas para considerar que los datos buscados están almacenados en otro sistema informático o en una parte de él, podrán ampliar el registro, siempre que los datos sean lícitamente accesibles por medio del sistema inicial o estén disponibles para este. Esta ampliación del registro deberá ser autorizada por el juez, salvo que ya lo hubiera sido en la autorización inicial. En caso de urgencia, la Policía Judicial o el fiscal podrán llevarlo a cabo, informando al juez inmediatamente, y en todo caso dentro del plazo máximo de veinticuatro horas, de la

actuación realizada, la forma en que se ha efectuado y su resultado. El juez competente, también de forma motivada, revocará o confirmará tal actuación en un plazo máximo de setenta y dos horas desde que fue ordenada la interceptación.

4. En los casos de urgencia en que se aprecie un interés constitucional legítimo que haga imprescindible la medida prevista en los apartados anteriores de este artículo, la Policía Judicial podrá llevar a cabo el examen directo de los datos contenidos en el dispositivo incautado, comunicándolo inmediatamente, y en todo caso dentro del plazo máximo de veinticuatro horas, por escrito motivado al juez competente, haciendo constar las razones que justificaron la adopción de la medida, la actuación realizada, la forma en que se ha efectuado y su resultado. El juez competente, también de forma motivada, revocará o confirmará tal actuación en un plazo máximo de 72 horas desde que fue ordenada la medida.

5. Las autoridades y agentes encargados de la investigación podrán ordenar a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo que facilite la información que resulte necesaria, siempre que de ello no derive una carga desproporcionada para el afectado, bajo apercibimiento de incurrir en delito de desobediencia.

Esta disposición no será aplicable al investigado o encausado, a las personas que están dispensadas de la obligación de declarar por razón de parentesco y a aquellas que, de conformidad con el artículo 416.2, no pueden declarar en virtud del secreto profesional.

CAPÍTULO IX

Registros remotos sobre equipos informáticos

Artículo 588 septies a. *Presupuestos.*

1. El juez competente podrá autorizar la utilización de datos de identificación y códigos, así como la instalación de un software, que permitan, de forma remota y telemática, el examen a distancia y sin conocimiento de su titular o usuario del contenido de un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos informáticos o base de datos, siempre que persiga la investigación de alguno de los siguientes delitos:

a) Delitos cometidos en el seno de organizaciones criminales.

b) Delitos de terrorismo.

c) Delitos cometidos contra menores o personas con capacidad modificada judicialmente.

d) Delitos contra la Constitución, de traición y relativos a la defensa nacional.

e) Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación.

2. La resolución judicial que autorice el registro deberá especificar:

a) Los ordenadores, dispositivos electrónicos, sistemas informáticos o parte de los mismos, medios informáticos de almacenamiento de datos o bases de datos, datos u otros contenidos digitales objeto de la medida.

b) El alcance de la misma, la forma en la que se procederá al acceso y aprehensión de los datos o archivos informáticos relevantes para la causa y el software mediante el que se ejecutará el control de la información.

c) Los agentes autorizados para la ejecución de la medida.

d) La autorización, en su caso, para la realización y conservación de copias de los datos informáticos.

e) Las medidas precisas para la preservación de la integridad de los datos almacenados, así como para la inaccesibilidad o supresión de dichos datos del sistema informático al que se ha tenido acceso.

3. Cuando los agentes que lleven a cabo el registro remoto tengan razones para creer que los datos buscados están almacenados en otro sistema informático o en una parte del

mismo, pondrán este hecho en conocimiento del juez, quien podrá autorizar una ampliación de los términos del registro.

Artículo 588 septies b. *Deber de colaboración.*

1. Los prestadores de servicios y personas señaladas en el artículo 588 ter e y los titulares o responsables del sistema informático o base de datos objeto del registro están obligados a facilitar a los agentes investigadores la colaboración precisa para la práctica de la medida y el acceso al sistema. Asimismo, están obligados a facilitar la asistencia necesaria para que los datos e información recogidos puedan ser objeto de examen y visualización.

2. Las autoridades y los agentes encargados de la investigación podrán ordenar a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo que facilite la información que resulte necesaria para el buen fin de la diligencia.

Esta disposición no será aplicable al investigado o encausado, a las personas que están dispensadas de la obligación de declarar por razón de parentesco, y a aquellas que, de conformidad con el artículo 416.2, no pueden declarar en virtud del secreto profesional.

3. Los sujetos requeridos para prestar colaboración tendrán la obligación de guardar secreto acerca de las actividades requeridas por las autoridades.

4. Los sujetos mencionados en los apartados 1 y 2 de este artículo quedarán sujetos a la responsabilidad regulada en el apartado 3 del artículo 588 ter e.

Artículo 588 septies c. *Duración.*

La medida tendrá una duración máxima de un mes, prorrogable por iguales períodos hasta un máximo de tres meses.

CAPÍTULO X

Medidas de aseguramiento

Artículo 588 octies. *Orden de conservación de datos.*

El Ministerio Fiscal o la Policía Judicial podrán requerir a cualquier persona física o jurídica la conservación y protección de datos o informaciones concretas incluidas en un sistema informático de almacenamiento que se encuentren a su disposición hasta que se obtenga la autorización judicial correspondiente para su cesión con arreglo a lo dispuesto en los artículos precedentes.

Los datos se conservarán durante un periodo máximo de noventa días, prorrogable una sola vez hasta que se autorice la cesión o se cumplan ciento ochenta días.

El requerido vendrá obligado a prestar su colaboración y a guardar secreto del desarrollo de esta diligencia, quedando sujeto a la responsabilidad descrita en el apartado·3 del artículo 588 ter e.

[. . .]

TÍTULO III

De la celebración del juicio oral

[. . .]

CAPÍTULO III

Del modo de practicar las pruebas durante el juicio oral

[. . .]

Sección 3.ª Del informe pericial

Artículo 723.

Los peritos podrán ser recusados por las causas y en la forma prescrita en los artículos 468, 469 y 470.

La sustanciación de los incidentes de recusación tendrá lugar precisamente en el tiempo que media desde la admisión de las pruebas propuestas por las partes hasta la apertura de las sesiones.

Artículo 724.

Los peritos que no hayan sido recusados serán examinados juntos cuando deban declarar sobre unos mismos hechos, y contestarán a las preguntas y repreguntas que las partes les dirijan.

Artículo 725.

Si para contestarlas considerasen necesaria la práctica de cualquier reconocimiento, harán éste, acto continuo, en el local de la misma audiencia si fuere posible.

En otro caso se suspenderá la sesión por el tiempo necesario, a no ser que puedan continuar practicándose otras diligencias de prueba entre tanto que los peritos verifican el reconocimiento.

Sección 4.ª De la prueba documental y de la inspección ocular

Artículo 726.

El Tribunal examinará por sí mismo los libros, documentos, papeles y demás piezas de convicción que puedan contribuir al esclarecimiento de los hechos o a la más segura investigación de la verdad.

Artículo 727.

Para la prueba de inspección ocular que no se haya practicado antes de la apertura de las sesiones, si el lugar que deba ser inspeccionado se hallase en la capital, se constituirá en él el Tribunal con las partes, y el Secretario extenderá diligencia expresiva del lugar o cosa inspeccionada, haciendo constar en ella las observaciones de las partes y demás incidentes que ocurran.

Si el lugar estuviere fuera de la capital, se constituirá en él con las partes el individuo del Tribunal que el Presidente designe, practicándose las diligencias en la forma establecida en el párrafo anterior.

En todo lo demás se estará, en cuanto fuere necesario, a lo dispuesto en el título V, capítulo I del libro II.

[. . .]

TÍTULO II

Del procedimiento abreviado

[. . .]

CAPÍTULO II

De las actuaciones de la Policía Judicial y del Ministerio Fiscal

Artículo 769.

Sin perjuicio de lo establecido en el Título III del Libro II de esta Ley, tan pronto como tenga conocimiento de un hecho que revista caracteres de delito, la Policía judicial observará las reglas establecidas en este capítulo.

Artículo 770.

La Policía Judicial acudirá de inmediato al lugar de los hechos y realizará las siguientes diligencias:

1.ª Requerirá la presencia de cualquier facultativo o personal sanitario que fuere habido para prestar, si fuere necesario, los oportunos auxilios al ofendido. El requerido, aunque sólo lo fuera verbalmente, que no atienda sin justa causa el requerimiento será sancionado con una multa de 500 a 5.000 euros, sin perjuicio de la responsabilidad criminal en que hubiera podido incurrir.

2.ª Acompañará al acta de constancia fotografías o cualquier otro soporte magnético o de reproducción de la imagen, cuando sea pertinente para el esclarecimiento del hecho punible y exista riesgo de desaparición de sus fuentes de prueba.

3.ª Recogerá y custodiará en todo caso los efectos, instrumentos o pruebas del delito de cuya desaparición hubiere peligro, para ponerlos a disposición de la autoridad judicial.

4.ª Si se hubiere producido la muerte de alguna persona y el cadáver se hallare en la vía pública, en la vía férrea o en otro lugar de tránsito, lo trasladará al lugar próximo que resulte más idóneo dentro de las circunstancias, restableciendo el servicio interrumpido y dando cuenta de inmediato a la autoridad judicial. En las situaciones excepcionales en que haya de adoptarse tal medida de urgencia, se reseñará previamente la posición del interfecto, obteniéndose fotografías y señalando sobre el lugar la situación exacta que ocupaba.

5.ª Tomará los datos personales y dirección de las personas que se encuentren en el lugar en que se cometió el hecho, así como cualquier otro dato que ayude a su identificación y localización, tales como lugar habitual de trabajo, números de teléfono fijo o móvil, número de fax o dirección de correo electrónico.

6.ª Intervendrá, de resultar procedente, el vehículo y retendrá el permiso de circulación del mismo y el permiso de conducir de la persona a la que se impute el hecho.

Artículo 771.

En el tiempo imprescindible y, en todo caso, durante el tiempo de la detención, si la hubiere, la Policía Judicial practicará las siguientes diligencias:

1.ª Cumplirá con los deberes de información a las víctimas que prevé la legislación vigente. En particular, informará al ofendido y al perjudicado por el delito de forma escrita de los derechos que les asisten de acuerdo con lo establecido en los artículos 109 y 110. Se instruirá al ofendido de su derecho a mostrarse parte en la causa sin necesidad de formular querella y, tanto al ofendido como al perjudicado, de su derecho a nombrar Abogado o instar el nombramiento de Abogado de oficio en caso de ser titulares del derecho a la asistencia jurídica gratuita, de su derecho a, una vez personados en la causa, tomar conocimiento de lo actuado, sin perjuicio de lo dispuesto en los artículos 301 y 302, e instar lo que a su derecho convenga. Asimismo, se les informará de que, de no personarse en la causa y no hacer renuncia ni reserva de acciones civiles, el Ministerio Fiscal las ejercitará si correspondiere.

Informará asimismo a la persona ofendida o perjudicada de que puede optar por relacionarse con la Administración de Justicia por los medios del artículo 162 de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, recabando y consignando sucintamente su respuesta.

La información de derechos al ofendido o perjudicado regulada en este artículo, cuando se refiera a los delitos contra la propiedad intelectual o industrial, y, en su caso, su citación o emplazamiento en los distintos trámites del proceso, se realizará a aquellas personas, entidades u organizaciones que ostenten la representación legal de los titulares de dichos derechos.

2.ª Informará en la forma más comprensible al investigado no detenido de cuáles son los hechos que se le atribuyen y de los derechos que le asisten. En particular, le instruirá de los derechos reconocidos en los apartados a), b), c) y e) del artículo 520.2.

Téngase en cuenta que esta actualización, que añade el párrafo segundo a la diligencia 1º, establecida por el art. 20.7 de la Ley Orgánica 1/2025, de 2 de enero. Ref. BOE-A-2025-76, entra en vigor el 3 de abril de 2025, según determina su disposición final 38.1.

Artículo 772.

1. Los miembros de la Policía Judicial requerirán el auxilio de otros miembros de las Fuerzas y Cuerpos de Seguridad cuando fuera necesario para el desempeño de las funciones que por esta Ley se les encomiendan.

2. La Policía extenderá el atestado de acuerdo con las normas generales de esta Ley y lo entregará al Juzgado competente, pondrá a su disposición a los detenidos, si los hubiere, y remitirá copia al Ministerio Fiscal.

Artículo 773.

1. El Fiscal se constituirá en las actuaciones para el ejercicio de las acciones penal y civil conforme a la Ley. Velará por el respeto de las garantías procesales del investigado o encausado y por la protección de los derechos de la víctima y de los perjudicados por el delito.

En este procedimiento corresponde al Ministerio Fiscal, de manera especial, impulsar y simplificar su tramitación sin merma del derecho de defensa de las partes y del carácter contradictorio del mismo, dando a la Policía Judicial instrucciones generales o particulares para el más eficaz cumplimiento de sus funciones, interviniendo en las actuaciones, aportando los medios de prueba de que pueda disponer o solicitando del Juez de Instrucción la práctica de los mismos, así como instar de éste la adopción de medidas cautelares o su levantamiento y la conclusión de la investigación tan pronto como estime que se han practicado las actuaciones necesarias para resolver sobre el ejercicio de la acción penal.

El Fiscal General del Estado impartirá cuantas órdenes e instrucciones estime convenientes respecto a la actuación del Fiscal en este procedimiento, y en especial, respecto a la aplicación de lo dispuesto en el apartado 1 del artículo 780.

Tan pronto como el Juez ordene la incoación del procedimiento para las causas ante el Tribunal del Jurado, el Secretario judicial lo pondrá en conocimiento del Ministerio Fiscal, quien comparecerá e intervendrá en cuantas actuaciones se lleven a cabo ante aquél.

2. Cuando el Ministerio Fiscal tenga noticia de un hecho aparentemente delictivo, bien directamente o por serle presentada una denuncia o atestado, informará a la víctima de los derechos recogidos en la legislación vigente; efectuará la evaluación y resolución provisionales de las necesidades de la víctima de conformidad con lo dispuesto en la legislación vigente y practicará él mismo u ordenará a la Policía Judicial que practique las diligencias que estime pertinentes para la comprobación del hecho o de la responsabilidad de los partícipes en el mismo. El Fiscal decretará el archivo de las actuaciones cuando el hecho no revista los caracteres de delito, comunicándolo con expresión de esta circunstancia a quien hubiere alegado ser perjudicado u ofendido, a fin de que pueda reiterar su denuncia ante el Juez de Instrucción. En otro caso instará del Juez de Instrucción la incoación del procedimiento que corresponda con remisión de lo actuado, poniendo a su disposición al detenido, si lo hubiere, y los efectos del delito.

El Ministerio Fiscal podrá hacer comparecer ante sí a cualquier persona en los términos establecidos en la ley para la citación judicial, a fin de recibirle declaración, en la cual se observarán las mismas garantías señaladas en esta Ley para la prestada ante el Juez o Tribunal.

Cesará el Fiscal en sus diligencias tan pronto como tenga conocimiento de la existencia de un procedimiento judicial sobre los mismos hechos.

[. . .]

TÍTULO V

Del procedimiento por delitos cometidos por medio de la imprenta, el grabado u otro medio mecánico de publicación

Artículo 816.

Inmediatamente que se dé principio a un procedimiento por delito cometido por medio de la imprenta, el grabado u otro medio mecánico de publicación, el Juez o Tribunal acordará el secuestro de los ejemplares del impreso o de la estampa donde quiera que se hallaren y del molde de ésta.

Se procederá, asimismo, inmediatamente a averiguar quién haya sido el autor real del escrito o estampa con cuya publicación se hubiese cometido el delito.

Artículo 817.

Si el escrito o estampa se hubiese publicado en periódico, bien en el texto del mismo, bien en hoja aparte, se tomará declaración para averiguar quién haya sido el autor al Director o redactores de aquél y al Jefe o Regente del establecimiento tipográfico en que se haya hecho la impresión o grabado.

Para ello se reclamará el original de cualquiera de las personas que lo tenga en su poder, la cual, si no lo pusiere a disposición del Juez, manifestará la persona a quien lo haya entregado.

Artículo 818.

Si el delito se hubiese cometido por medio de la publicación de un escrito o de una estampa sueltos, se tomará la declaración expresada en el artículo anterior al Jefe y dependientes del establecimiento en que se haya hecho la impresión o estampación.

Artículo 819.

Cuando no pudiere averiguarse quién sea el autor real del escrito o estampa, o cuando por hallarse domiciliado en el extranjero o por cualquier otra causa de las especificadas en el Código Penal no pudiere ser perseguido, se dirigirá el procedimiento contra las personas subsidiariamente responsables, por el orden establecido en el artículo respectivo del expresado Código.

Artículo 820.

No será bastante la confesión de un supuesto autor para que se le tenga como tal y para que no se dirija el procedimiento contra otras personas, si de las circunstancias de aquél o de las del delito resultaren indicios bastantes para creer que el confeso no fue el autor real del escrito o estampa publicados.

Pero una vez dictada sentencia firme en contra de los subsidiariamente responsables, no se podrá abrir nuevo procedimiento contra el responsable principal si llegare a ser conocido.

Artículo 821.

Si durante el curso de la causa apareciere alguna persona que, por el orden establecido en el artículo respectivo del Código Penal, deba responder criminalmente del delito antes que el procesado, se sobreseerá la causa respecto a éste, dirigiéndose el procedimiento contra aquélla.

Artículo 822.

No se considerarán como instrumentos o efectos del delito más que los ejemplares impresos del escrito o estampa y el molde de ésta.

Artículo 823.

Unidos a la causa el impreso, grabado u otro medio mecánico de publicación que haya servido para la comisión del delito, y averiguado el autor o la persona subsidiariamente responsable, se dará por terminado el sumario.

Artículo 823 bis.

Las normas del presente título serán también aplicables al enjuiciamiento de los delitos cometidos a través de medios sonoros o fotográficos, difundidos por escrito, radio, televisión, cinematógrafo u otros similares.

Los Jueces, al iniciar el procedimiento, podrán acordar, según los casos, el secuestro de la publicación o la prohibición de difundir o proyectar el medio a través del cual se produjo la actividad delictiva. Contra dicha resolución podrá interponerse directamente recurso de apelación, que deberá ser resuelto en el plazo de cinco días.

[. . .]

§ 51

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

Jefatura del Estado
«BOE» núm. 294, de 6 de diciembre de 2018
Última modificación: 9 de mayo de 2023
Referencia: BOE-A-2018-16673

FELIPE VI

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley orgánica.

PREÁMBULO

I

La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental protegido por el artículo 18.4 de la Constitución española. De esta manera, nuestra Constitución fue pionera en el reconocimiento del derecho fundamental a la protección de datos personales cuando dispuso que «la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos». Se hacía así eco de los trabajos desarrollados desde finales de la década de 1960 en el Consejo de Europa y de las pocas disposiciones legales adoptadas en países de nuestro entorno.

El Tribunal Constitucional señaló en su Sentencia 94/1998, de 4 de mayo, que nos encontramos ante un derecho fundamental a la protección de datos por el que se garantiza a la persona el control sobre sus datos, cualesquiera datos personales, y sobre su uso y destino, para evitar el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados; de esta forma, el derecho a la protección de datos se configura como una facultad del ciudadano para oponerse a que determinados datos personales sean usados para fines distintos a aquel que justificó su obtención. Por su parte, en la Sentencia 292/2000, de 30 de noviembre, lo considera como un derecho autónomo e independiente que consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso.

A nivel legislativo, la concreción y desarrollo del derecho fundamental de protección de las personas físicas en relación con el tratamiento de datos personales tuvo lugar en sus

orígenes mediante la aprobación de la Ley Orgánica 5/1992, de 29 de octubre, reguladora del tratamiento automatizado de datos personales, conocida como LORTAD. La Ley Orgánica 5/1992 fue reemplazada por la Ley Orgánica 15/1999, de 5 de diciembre, de protección de datos personales, a fin de trasponer a nuestro derecho a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Esta ley orgánica supuso un segundo hito en la evolución de la regulación del derecho fundamental a la protección de datos en España y se complementó con una cada vez más abundante jurisprudencia procedente de los órganos de la jurisdicción contencioso-administrativa.

Por otra parte, también se recoge en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea y en el artículo 16.1 del Tratado de Funcionamiento de la Unión Europea. Anteriormente, a nivel europeo, se había adoptado la Directiva 95/46/CE citada, cuyo objeto era procurar que la garantía del derecho a la protección de datos personales no supusiese un obstáculo a la libre circulación de los datos en el seno de la Unión, estableciendo así un espacio común de garantía del derecho que, al propio tiempo, asegurase que en caso de transferencia internacional de los datos, su tratamiento en el país de destino estuviese protegido por salvaguardas adecuadas a las previstas en la propia directiva.

II

En los últimos años de la pasada década se intensificaron los impulsos tendentes a lograr una regulación más uniforme del derecho fundamental a la protección de datos en el marco de una sociedad cada vez más globalizada. Así, se fueron adoptando en distintas instancias internacionales propuestas para la reforma del marco vigente. Y en este marco la Comisión lanzó el 4 de noviembre de 2010 su Comunicación titulada «Un enfoque global de la protección de los datos personales en la Unión Europea», que constituye el germen de la posterior reforma del marco de la Unión Europea. Al propio tiempo, el Tribunal de Justicia de la Unión ha venido adoptando a lo largo de los últimos años una jurisprudencia que resulta fundamental en su interpretación.

El último hito en esta evolución tuvo lugar con la adopción del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), así como de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

III

El Reglamento general de protección de datos pretende con su eficacia directa superar los obstáculos que impidieron la finalidad armonizadora de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos. La transposición de la directiva por los Estados miembros se ha plasmado en un mosaico normativo con perfiles irregulares en el conjunto de la Unión Europea lo que, en último extremo, ha conducido a que existan diferencias apreciables en la protección de los derechos de los ciudadanos.

Asimismo, se atiende a nuevas circunstancias, principalmente el aumento de los flujos transfronterizos de datos personales como consecuencia del funcionamiento del mercado interior, los retos planteados por la rápida evolución tecnológica y la globalización, que ha hecho que los datos personales sean el recurso fundamental de la sociedad de la información. El carácter central de la información personal tiene aspectos positivos, porque permite nuevos y mejores servicios, productos o hallazgos científicos. Pero tiene también

riesgos, pues las informaciones sobre los individuos se multiplican exponencialmente, son más accesibles, por más actores, y cada vez son más fáciles de procesar mientras que es más difícil el control de su destino y uso.

El Reglamento general de protección de datos supone la revisión de las bases legales del modelo europeo de protección de datos más allá de una mera actualización de la vigente normativa. Procede a reforzar la seguridad jurídica y transparencia a la vez que permite que sus normas sean especificadas o restringidas por el Derecho de los Estados miembros en la medida en que sea necesario por razones de coherencia y para que las disposiciones nacionales sean comprensibles para sus destinatarios. Así, el Reglamento general de protección de datos contiene un buen número de habilitaciones, cuando no imposiciones, a los Estados miembros, a fin de regular determinadas materias, permitiendo incluso en su considerando 8, y a diferencia de lo que constituye principio general del Derecho de la Unión Europea que, cuando sus normas deban ser especificadas, interpretadas o, excepcionalmente, restringidas por el Derecho de los Estados miembros, estos tengan la posibilidad de incorporar al derecho nacional previsiones contenidas específicamente en el reglamento, en la medida en que sea necesario por razones de coherencia y comprensión.

En este punto hay que subrayar que no se excluye toda intervención del Derecho interno en los ámbitos concernidos por los reglamentos europeos. Al contrario, tal intervención puede ser procedente, incluso necesaria, tanto para la depuración del ordenamiento nacional como para el desarrollo o complemento del reglamento de que se trate. Así, el principio de seguridad jurídica, en su vertiente positiva, obliga a los Estados miembros a integrar el ordenamiento europeo en el interno de una manera lo suficientemente clara y pública como para permitir su pleno conocimiento tanto por los operadores jurídicos como por los propios ciudadanos, en tanto que, en su vertiente negativa, implica la obligación para tales Estados de eliminar situaciones de incertidumbre derivadas de la existencia de normas en el Derecho nacional incompatibles con el europeo. De esta segunda vertiente se colige la consiguiente obligación de depurar el ordenamiento jurídico. En definitiva, el principio de seguridad jurídica obliga a que la normativa interna que resulte incompatible con el Derecho de la Unión Europea quede definitivamente eliminada «mediante disposiciones internas de carácter obligatorio que tengan el mismo valor jurídico que las disposiciones internas que deban modificarse» (Sentencias del Tribunal de Justicia de 23 de febrero de 2006, asunto Comisión vs. España; de 13 de julio de 2000, asunto Comisión vs. Francia; y de 15 de octubre de 1986, asunto Comisión vs. Italia). Por último, los reglamentos, pese a su característica de aplicabilidad directa, en la práctica pueden exigir otras normas internas complementarias para hacer plenamente efectiva su aplicación. En este sentido, más que de incorporación cabría hablar de «desarrollo» o complemento del Derecho de la Unión Europea.

La adaptación al Reglamento general de protección de datos, que será aplicable a partir del 25 de mayo de 2018, según establece su artículo 99, requiere, en suma, la elaboración de una nueva ley orgánica que sustituya a la actual. En esta labor se han preservado los principios de buena regulación, al tratarse de una norma necesaria para la adaptación del ordenamiento español a la citada disposición europea y proporcional a este objetivo, siendo su razón última procurar seguridad jurídica.

IV

Internet, por otra parte, se ha convertido en una realidad omnipresente tanto en nuestra vida personal como colectiva. Una gran parte de nuestra actividad profesional, económica y privada se desarrolla en la Red y adquiere una importancia fundamental tanto para la comunicación humana como para el desarrollo de nuestra vida en sociedad. Ya en los años noventa, y conscientes del impacto que iba a producir Internet en nuestras vidas, los pioneros de la Red propusieron elaborar una Declaración de los Derechos del Hombre y del Ciudadano en Internet.

Hoy identificamos con bastante claridad los riesgos y oportunidades que el mundo de las redes ofrece a la ciudadanía. Corresponde a los poderes públicos impulsar políticas que hagan efectivos los derechos de la ciudadanía en Internet promoviendo la igualdad de los ciudadanos y de los grupos en los que se integran para hacer posible el pleno ejercicio de los derechos fundamentales en la realidad digital. La transformación digital de nuestra

sociedad es ya una realidad en nuestro desarrollo presente y futuro tanto a nivel social como económico. En este contexto, países de nuestro entorno ya han aprobado normativa que refuerza los derechos digitales de la ciudadanía.

Los constituyentes de 1978 ya intuyeron el enorme impacto que los avances tecnológicos provocarían en nuestra sociedad y, en particular, en el disfrute de los derechos fundamentales. Una deseable futura reforma de la Constitución debería incluir entre sus prioridades la actualización de la Constitución a la era digital y, específicamente, elevar a rango constitucional una nueva generación de derechos digitales. Pero, en tanto no se acometa este reto, el legislador debe abordar el reconocimiento de un sistema de garantía de los derechos digitales que, inequívocamente, encuentra su anclaje en el mandato impuesto por el apartado cuarto del artículo 18 de la Constitución Española y que, en algunos casos, ya han sido perfilados por la jurisprudencia ordinaria, constitucional y europea.

V

Esta ley orgánica consta de noventa y siete artículos estructurados en diez títulos, veintidós disposiciones adicionales, seis disposiciones transitorias, una disposición derogatoria y dieciséis disposiciones finales.

El Título I, relativo a las disposiciones generales, comienza regulando el objeto de la ley orgánica, que es, conforme a lo que se ha indicado, doble. Así, en primer lugar, se pretende lograr la adaptación del ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, Reglamento general de protección de datos, y completar sus disposiciones. A su vez, establece que el derecho fundamental de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento (UE) 2016/679 y en esta ley orgánica. Las comunidades autónomas ostentan competencias de desarrollo normativo y ejecución del derecho fundamental a la protección de datos personales en su ámbito de actividad y a las autoridades autonómicas de protección de datos que se creen les corresponde contribuir a garantizar este derecho fundamental de la ciudadanía. En segundo lugar, es también objeto de la ley garantizar los derechos digitales de la ciudadanía, al amparo de lo dispuesto en el artículo 18.4 de la Constitución.

Destaca la novedosa regulación de los datos referidos a las personas fallecidas, pues, tras excluir del ámbito de aplicación de la ley su tratamiento, se permite que las personas vinculadas al fallecido por razones familiares o de hecho o sus herederos puedan solicitar el acceso a los mismos, así como su rectificación o supresión, en su caso con sujeción a las instrucciones del fallecido. También excluye del ámbito de aplicación los tratamientos que se rijan por disposiciones específicas, en referencia, entre otras, a la normativa que transponga la citada Directiva (UE) 2016/680, previéndose en la disposición transitoria cuarta la aplicación a estos tratamientos de la Ley Orgánica 15/1999, de 13 de diciembre, hasta que se apruebe la citada normativa.

En el Título II, «Principios de protección de datos», se establece que a efectos del Reglamento (UE) 2016/679 no serán imputables al responsable del tratamiento, siempre que este haya adoptado todas las medidas razonables para que se supriman o rectifiquen sin dilación, la inexactitud de los datos obtenidos directamente del afectado, cuando hubiera recibido los datos de otro responsable en virtud del ejercicio por el afectado del derecho a la portabilidad, o cuando el responsable los obtuviese del mediador o intermediario cuando las normas aplicables al sector de actividad al que pertenezca el responsable del tratamiento establezcan la posibilidad de intervención de un intermediario o mediador o cuando los datos hubiesen sido obtenidos de un registro público. También se recoge expresamente el deber de confidencialidad, el tratamiento de datos amparado por la ley, las categorías especiales de datos y el tratamiento de datos de naturaleza penal, se alude específicamente al consentimiento, que ha de proceder de una declaración o de una clara acción afirmativa del afectado, excluyendo lo que se conocía como «consentimiento tácito», se indica que el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que se otorga para todas ellas, y se mantiene en catorce años la edad a partir de la cual el menor puede prestar su consentimiento.

Se regulan asimismo las posibles habilitaciones legales para el tratamiento fundadas en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el Reglamento (UE) 2016/679, cuando así lo prevea una norma de Derecho de la Unión Europea o una ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal, Este es el caso, por ejemplo, de las bases de datos reguladas por ley y gestionadas por autoridades públicas que responden a objetivos específicos de control de riesgos y solvencia, supervisión e inspección del tipo de la Central de Información de Riesgos del Banco de España regulada por la Ley 44/2002, de 22 de noviembre, de Medidas de Reforma del Sistema Financiero, o de los datos, documentos e informaciones de carácter reservado que obren en poder de la Dirección General de Seguros y Fondos de Pensiones de conformidad con lo previsto en la Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.

Se podrán igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras, cuando ello derive del ejercicio de potestades públicas o del cumplimiento de una obligación legal y solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el reglamento europeo, cuando derive de una competencia atribuida por la ley. Y se mantiene la prohibición de consentir tratamientos con la finalidad principal de almacenar información identificativa de determinadas categorías de datos especialmente protegidos, lo que no impide que los mismos puedan ser objeto de tratamiento en los demás supuestos previstos en el Reglamento (UE) 2016/679. Así, por ejemplo, la prestación del consentimiento no dará cobertura a la creación de «listas negras» de sindicalistas, si bien los datos de afiliación sindical podrán ser tratados por el empresario para hacer posible el ejercicio de los derechos de los trabajadores al amparo del artículo 9.2.b) del Reglamento (UE) 2016/679 o por los propios sindicatos en los términos del artículo 9.2.d) de la misma norma europea.

También en relación con el tratamiento de categorías especiales de datos, el artículo 9.2 consagra el principio de reserva de ley para su habilitación en los supuestos previstos en el Reglamento (UE) 2016/679. Dicha previsión no sólo alcanza a las disposiciones que pudieran adoptarse en el futuro, sino que permite dejar a salvo las distintas habilitaciones legales actualmente existentes, tal y como se indica específicamente, respecto de la legislación sanitaria y aseguradora, en la disposición adicional decimoséptima. El Reglamento general de protección de datos no afecta a dichas habilitaciones, que siguen plenamente vigentes, permitiendo incluso llevar a cabo una interpretación extensiva de las mismas, como sucede, en particular, en cuanto al alcance del consentimiento del afectado o el uso de sus datos sin consentimiento en el ámbito de la investigación biomédica. A tal efecto, el apartado 2 de la Disposición adicional decimoséptima introduce una serie de previsiones encaminadas a garantizar el adecuado desarrollo de la investigación en materia de salud, y en particular la biomédica, ponderando los indudables beneficios que la misma aporta a la sociedad con las debidas garantías del derecho fundamental a la protección de datos.

El Título III, dedicado a los derechos de las personas, adapta al Derecho español el principio de transparencia en el tratamiento del reglamento europeo, que regula el derecho de los afectados a ser informados acerca del tratamiento y recoge la denominada «información por capas» ya generalmente aceptada en ámbitos como el de la videovigilancia o la instalación de dispositivos de almacenamiento masivo de datos (tales como las «cookies»), facilitando al afectado la información básica, si bien, indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

Se hace uso en este Título de la habilitación permitida por el considerando 8 del Reglamento (UE) 2016/679 para complementar su régimen, garantizando la adecuada estructura sistemática del texto. A continuación, la ley orgánica contempla los derechos de acceso, rectificación, supresión, oposición, derecho a la limitación del tratamiento y derecho a la portabilidad.

En el Título IV se recogen «Disposiciones aplicables a tratamientos concretos», incorporando una serie de supuestos que en ningún caso debe considerarse exhaustiva de

todos los tratamientos lícitos. Dentro de ellos cabe apreciar, en primer lugar, aquellos respecto de los que el legislador establece una presunción «iuris tantum» de prevalencia del interés legítimo del responsable cuando se lleven a cabo con una serie de requisitos, lo que no excluye la licitud de este tipo de tratamientos cuando no se cumplen estrictamente las condiciones previstas en el texto, si bien en este caso el responsable deberá llevar a cabo la ponderación legalmente exigible, al no presumirse la prevalencia de su interés legítimo. Junto a estos supuestos se recogen otros, tales como la videovigilancia, los ficheros de exclusión publicitaria o los sistemas de denuncias internas en que la licitud del tratamiento proviene de la existencia de un interés público, en los términos establecidos en el artículo 6.1.e) del Reglamento (UE) 2016/679. Finalmente, se hace referencia en este Título a la licitud de otros tratamientos regulados en el Capítulo IX del reglamento, como los relacionados con la función estadística o con fines de archivo de interés general. En todo caso, el hecho de que el legislador se refiera a la licitud de los tratamientos no enerva la obligación de los responsables de adoptar todas las medidas de responsabilidad activa establecidas en el Capítulo IV del reglamento europeo y en el Título V de esta ley orgánica.

El Título V se refiere al responsable y al encargado del tratamiento. Es preciso tener en cuenta que la mayor novedad que presenta el Reglamento (UE) 2016/679 es la evolución de un modelo basado, fundamentalmente, en el control del cumplimiento a otro que descansa en el principio de responsabilidad activa, lo que exige una previa valoración por el responsable o por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos personales para, a partir de dicha valoración, adoptar las medidas que procedan. Con el fin de aclarar estas novedades, la ley orgánica mantiene la misma denominación del Capítulo IV del Reglamento, dividiendo el articulado en cuatro capítulos dedicados, respectivamente, a las medidas generales de responsabilidad activa, al régimen del encargado del tratamiento, a la figura del delegado de protección de datos y a los mecanismos de autorregulación y certificación. La figura del delegado de protección de datos adquiere una destacada importancia en el Reglamento (UE) 2016/679 y así lo recoge la ley orgánica, que parte del principio de que puede tener un carácter obligatorio o voluntario, estar o no integrado en la organización del responsable o encargado y ser tanto una persona física como una persona jurídica. La designación del delegado de protección de datos ha de comunicarse a la autoridad de protección de datos competente. La Agencia Española de Protección de Datos mantendrá una relación pública y actualizada de los delegados de protección de datos, accesible por cualquier persona. Los conocimientos en la materia se podrán acreditar mediante esquemas de certificación. Asimismo, no podrá ser removido, salvo en los supuestos de dolo o negligencia grave. Es de destacar que el delegado de protección de datos permite configurar un medio para la resolución amistosa de reclamaciones, pues el interesado podrá reproducir ante él la reclamación que no sea atendida por el responsable o encargado del tratamiento.

El Título VI, relativo a las transferencias internacionales de datos, procede a la adaptación de lo previsto en el Reglamento (UE) 2016/679 y se refiere a las especialidades relacionadas con los procedimientos a través de los cuales las autoridades de protección de datos pueden aprobar modelos contractuales o normas corporativas vinculantes, supuestos de autorización de una determinada transferencia, o información previa.

El Título VII se dedica a las autoridades de protección de datos, que siguiendo el mandato del Reglamento (UE) 2016/679 se han de establecer por ley nacional. Manteniendo el esquema que se venía recogiendo en sus antecedentes normativos, la ley orgánica regula el régimen de la Agencia Española de Protección de Datos y refleja la existencia de las autoridades autonómicas de protección de datos y la necesaria cooperación entre las autoridades de control. La Agencia Española de Protección de Datos se configura como una autoridad administrativa independiente con arreglo a la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, que se relaciona con el Gobierno a través del Ministerio de Justicia.

El Título VIII regula el «Procedimientos en caso de posible vulneración de la normativa de protección de datos». El Reglamento (UE) 2016/679 establece un sistema novedoso y complejo, evolucionando hacia un modelo de «ventanilla única» en el que existe una autoridad de control principal y otras autoridades interesadas. También se establece un procedimiento de cooperación entre autoridades de los Estados miembros y, en caso de

discrepancia, se prevé la decisión vinculante del Comité Europeo de Protección de Datos. En consecuencia, con carácter previo a la tramitación de cualquier procedimiento, será preciso determinar si el tratamiento tiene o no carácter transfronterizo y, en caso de tenerlo, qué autoridad de protección de datos ha de considerarse principal.

La regulación se limita a delimitar el régimen jurídico; la iniciación de los procedimientos, siendo posible que la Agencia Española de Protección de Datos remita la reclamación al delegado de protección de datos o a los órganos o entidades que tengan a su cargo la resolución extrajudicial de conflictos conforme a lo establecido en un código de conducta; la inadmisión de las reclamaciones; las actuaciones previas de investigación; las medidas provisionales, entre las que destaca la orden de bloqueo de los datos; y el plazo de tramitación de los procedimientos y, en su caso, su suspensión. Las especialidades del procedimiento se remiten al desarrollo reglamentario.

El Título IX, que contempla el régimen sancionador, parte de que el Reglamento (UE) 2016/679 establece un sistema de sanciones o actuaciones correctivas que permite un amplio margen de apreciación. En este marco, la ley orgánica procede a describir las conductas típicas, estableciendo la distinción entre infracciones muy graves, graves y leves, tomando en consideración la diferenciación que el Reglamento general de protección de datos establece al fijar la cuantía de las sanciones. La categorización de las infracciones se introduce a los solos efectos de determinar los plazos de prescripción, teniendo la descripción de las conductas típicas como único objeto la enumeración de manera ejemplificativa de algunos de los actos sancionables que deben entenderse incluidos dentro de los tipos generales establecidos en la norma europea. La ley orgánica regula los supuestos de interrupción de la prescripción partiendo de la exigencia constitucional del conocimiento de los hechos que se imputan a la persona, pero teniendo en cuenta la problemática derivada de los procedimientos establecidos en el reglamento europeo, en función de si el procedimiento se tramita exclusivamente por la Agencia Española de Protección de Datos o si se acude al procedimiento coordinado del artículo 60 del Reglamento general de protección de datos.

El Reglamento (UE) 2016/679 establece amplios márgenes para la determinación de la cuantía de las sanciones. La ley orgánica aprovecha la cláusula residual del artículo 83.2 de la norma europea, referida a los factores agravantes o atenuantes, para aclarar que entre los elementos a tener en cuenta podrán incluirse los que ya aparecían en el artículo 45.4 y 5 de la Ley Orgánica 15/1999, y que son conocidos por los operadores jurídicos.

Finalmente, el Título X de esta ley acomete la tarea de reconocer y garantizar un elenco de derechos digitales de los ciudadanos conforme al mandato establecido en la Constitución. En particular, son objeto de regulación los derechos y libertades predicables al entorno de Internet como la neutralidad de la Red y el acceso universal o los derechos a la seguridad y educación digital así como los derechos al olvido, a la portabilidad y al testamento digital. Ocupa un lugar relevante el reconocimiento del derecho a la desconexión digital en el marco del derecho a la intimidad en el uso de dispositivos digitales en el ámbito laboral y la protección de los menores en Internet. Finalmente, resulta destacable la garantía de la libertad de expresión y el derecho a la aclaración de informaciones en medios de comunicación digitales.

Las disposiciones adicionales se refieren a cuestiones como las medidas de seguridad en el ámbito del sector público, protección de datos y transparencia y acceso a la información pública, cómputo de plazos, autorización judicial en materia de transferencias internacionales de datos, la protección frente a prácticas abusivas que pudieran desarrollar ciertos operadores, o los tratamientos de datos de salud, entre otras.

De conformidad con la disposición adicional decimocuarta, la normativa relativa a las excepciones y limitaciones en el ejercicio de los derechos que hubiese entrado en vigor con anterioridad a la fecha de aplicación del reglamento europeo y en particular los artículos 23 y 24 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, seguirá vigente en tanto no sea expresamente modificada, sustituida o derogada. La pervivencia de esta normativa supone la continuidad de las excepciones y limitaciones que en ella se contienen hasta que se produzca su reforma o abrogación, si bien referida a los derechos tal y como se regulan en el Reglamento (UE) 2016/679 y en esta ley orgánica. Así, por ejemplo, en virtud de la referida disposición adicional, las Administraciones

tributarias responsables de los ficheros de datos con trascendencia tributaria a que se refiere el artículo 95 de la Ley 58/2003, de 17 de diciembre, General Tributaria, podrán, en relación con dichos datos, denegar el ejercicio de los derechos a que se refieren los artículos 15 a 22 del Reglamento (UE) 2016/679, cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras.

Las disposiciones transitorias están dedicadas, entre otras cuestiones, al estatuto de la Agencia Española de Protección de Datos, el régimen transitorio de los procedimientos o los tratamientos sometidos a la Directiva (UE) 2016/680. Se recoge una disposición derogatoria y, a continuación, figuran las disposiciones finales sobre los preceptos con carácter de ley ordinaria, el título competencial y la entrada en vigor.

Asimismo, se introducen las modificaciones necesarias de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil y la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, la Ley Orgánica, 6/1985, de 1 de julio, del Poder Judicial, la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General, la Ley 14/1986, de 25 de abril, General de Sanidad, la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica y la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Finalmente, y en relación con la garantía de los derechos digitales, también se introducen modificaciones en la Ley Orgánica 2/2006, de 3 de mayo, de Educación, la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, así como en el Texto Refundido de la Ley del Estatuto de los Trabajadores y en el Texto Refundido de la Ley del Estatuto Básico del Empleado Público.

TÍTULO I

Disposiciones generales

Artículo 1. *Objeto de la ley.*

La presente ley orgánica tiene por objeto:

a) Adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, y completar sus disposiciones.

El derecho fundamental de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento (UE) 2016/679 y en esta ley orgánica.

b) Garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución.

Artículo 2. *Ámbito de aplicación de los Títulos I a IX y de los artículos 89 a 94.*

1. Lo dispuesto en los Títulos I a IX y en los artículos 89 a 94 de la presente ley orgánica se aplica a cualquier tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.

2. Esta ley orgánica no será de aplicación:

a) A los tratamientos excluidos del ámbito de aplicación del Reglamento general de protección de datos por su artículo 2.2, sin perjuicio de lo dispuesto en los apartados 3 y 4 de este artículo.

b) A los tratamientos de datos de personas fallecidas, sin perjuicio de lo establecido en el artículo 3.

c) A los tratamientos sometidos a la normativa sobre protección de materias clasificadas.

3. Los tratamientos a los que no sea directamente aplicable el Reglamento (UE) 2016/679 por afectar a actividades no comprendidas en el ámbito de aplicación del Derecho de la Unión Europea, se regirán por lo dispuesto en su legislación específica si la hubiere y supletoriamente por lo establecido en el citado reglamento y en la presente ley orgánica. Se encuentran en esta situación, entre otros, los tratamientos realizados al amparo de la legislación orgánica del régimen electoral general, los tratamientos realizados en el ámbito de instituciones penitenciarias y los tratamientos derivados del Registro Civil, los Registros de la Propiedad y Mercantiles.

4. El tratamiento de datos llevado a cabo con ocasión de la tramitación por los órganos judiciales de los procesos de los que sean competentes, así como el realizado dentro de la gestión de la Oficina Judicial, se regirán por lo dispuesto en el Reglamento (UE) 2016/679 y la presente ley orgánica, sin perjuicio de las disposiciones de la Ley Orgánica 6/1985, de 1 julio, del Poder Judicial, que le sean aplicables.

5. El tratamiento de datos llevado a cabo con ocasión de la tramitación por el Ministerio Fiscal de los procesos de los que sea competente, así como el realizado con esos fines dentro de la gestión de la Oficina Fiscal, se regirán por lo dispuesto en el Reglamento (UE) 2016/679 y la presente Ley Orgánica, sin perjuicio de las disposiciones de la Ley 50/1981, de 30 de diciembre, reguladora del Estatuto Orgánico del Ministerio Fiscal, la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial y de las normas procesales que le sean aplicables.

Artículo 3. *Datos de las personas fallecidas.*

1. Las personas vinculadas al fallecido por razones familiares o de hecho así como sus herederos podrán dirigirse al responsable o encargado del tratamiento al objeto de solicitar el acceso a los datos personales de aquella y, en su caso, su rectificación o supresión.

Como excepción, las personas a las que se refiere el párrafo anterior no podrán acceder a los datos del causante, ni solicitar su rectificación o supresión, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley. Dicha prohibición no afectará al derecho de los herederos a acceder a los datos de carácter patrimonial del causante.

2. Las personas o instituciones a las que el fallecido hubiese designado expresamente para ello podrán también solicitar, con arreglo a las instrucciones recibidas, el acceso a los datos personales de este y, en su caso su rectificación o supresión.

Mediante real decreto se establecerán los requisitos y condiciones para acreditar la validez y vigencia de estos mandatos e instrucciones y, en su caso, el registro de los mismos.

3. En caso de fallecimiento de menores, estas facultades podrán ejercerse también por sus representantes legales o, en el marco de sus competencias, por el Ministerio Fiscal, que podrá actuar de oficio o a instancia de cualquier persona física o jurídica interesada.

En caso de fallecimiento de personas con discapacidad, estas facultades también podrán ejercerse, además de por quienes señala el párrafo anterior, por quienes hubiesen sido designados para el ejercicio de funciones de apoyo, si tales facultades se entendieran comprendidas en las medidas de apoyo prestadas por el designado.

TÍTULO II

Principios de protección de datos

Artículo 4. *Exactitud de los datos.*

1. Conforme al artículo 5.1.d) del Reglamento (UE) 2016/679 los datos serán exactos y, si fuere necesario, actualizados.

2. A los efectos previstos en el artículo 5.1.d) del Reglamento (UE) 2016/679, no será imputable al responsable del tratamiento, siempre que este haya adoptado todas las medidas razonables para que se supriman o rectifiquen sin dilación, la inexactitud de los datos personales, con respecto a los fines para los que se tratan, cuando los datos inexactos:

a) Hubiesen sido obtenidos por el responsable directamente del afectado.

b) Hubiesen sido obtenidos por el responsable de un mediador o intermediario en caso de que las normas aplicables al sector de actividad al que pertenezca el responsable del tratamiento establecieran la posibilidad de intervención de un intermediario o mediador que recoja en nombre propio los datos de los afectados para su transmisión al responsable. El mediador o intermediario asumirá las responsabilidades que pudieran derivarse en el supuesto de comunicación al responsable de datos que no se correspondan con los facilitados por el afectado.

c) Fuesen sometidos a tratamiento por el responsable por haberlos recibido de otro responsable en virtud del ejercicio por el afectado del derecho a la portabilidad conforme al artículo 20 del Reglamento (UE) 2016/679 y lo previsto en esta ley orgánica.

d) Fuesen obtenidos de un registro público por el responsable.

Artículo 5. *Deber de confidencialidad.*

1. Los responsables y encargados del tratamiento de datos así como todas las personas que intervengan en cualquier fase de este estarán sujetas al deber de confidencialidad al que se refiere el artículo 5.1.f) del Reglamento (UE) 2016/679.

2. La obligación general señalada en el apartado anterior será complementaria de los deberes de secreto profesional de conformidad con su normativa aplicable.

3. Las obligaciones establecidas en los apartados anteriores se mantendrán aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento.

Artículo 6. *Tratamiento basado en el consentimiento del afectado.*

1. De conformidad con lo dispuesto en el artículo 4.11 del Reglamento (UE) 2016/679, se entiende por consentimiento del afectado toda manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

2. Cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que dicho consentimiento se otorga para todas ellas.

3. No podrá supeditarse la ejecución del contrato a que el afectado consienta el tratamiento de los datos personales para finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual.

Artículo 7. *Consentimiento de los menores de edad.*

1. El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años.

Se exceptúan los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento.

2. El tratamiento de los datos de los menores de catorce años, fundado en el consentimiento, solo será lícito si consta el del titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o tutela.

Artículo 8. *Tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos.*

1. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el artículo 6.1.c) del Reglamento (UE) 2016/679, cuando así lo prevea una norma de Derecho de la Unión Europea o una norma con rango de ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal. Dicha norma podrá igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras establecidas en el capítulo IV del Reglamento (UE) 2016/679.

2. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos

conferidos al responsable, en los términos previstos en el artículo 6.1 e) del Reglamento (UE) 2016/679, cuando derive de una competencia atribuida por una norma con rango de ley.

Artículo 9. *Categorías especiales de datos.*

1. A los efectos del artículo 9.2.a) del Reglamento (UE) 2016/679, a fin de evitar situaciones discriminatorias, el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico.

Lo dispuesto en el párrafo anterior no impedirá el tratamiento de dichos datos al amparo de los restantes supuestos contemplados en el artículo 9.2 del Reglamento (UE) 2016/679, cuando así proceda.

2. Los tratamientos de datos contemplados en las letras g), h) e i) del artículo 9.2 del Reglamento (UE) 2016/679 fundados en el Derecho español deberán estar amparados en una norma con rango de ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad.

En particular, dicha norma podrá amparar el tratamiento de datos en el ámbito de la salud cuando así lo exija la gestión de los sistemas y servicios de asistencia sanitaria y social, pública y privada, o la ejecución de un contrato de seguro del que el afectado sea parte.

Artículo 10. *Tratamiento de datos de naturaleza penal.*

1. El tratamiento de datos personales relativos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas, para fines distintos de los de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, solo podrá llevarse a cabo cuando se encuentre amparado en una norma de Derecho de la Unión, en esta ley orgánica o en otras normas de rango legal.

2. El registro completo de los datos referidos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas a que se refiere el artículo 10 del Reglamento (UE) 2016/679, podrá realizarse conforme con lo establecido en la regulación del Sistema de registros administrativos de apoyo a la Administración de Justicia.

3. Fuera de los supuestos señalados en los apartados anteriores, los tratamientos de datos referidos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas solo serán posibles cuando sean llevados a cabo por abogados y procuradores y tengan por objeto recoger la información facilitada por sus clientes para el ejercicio de sus funciones.

TÍTULO III

Derechos de las personas

CAPÍTULO I

Transparencia e información

Artículo 11. *Transparencia e información al afectado.*

1. Cuando los datos personales sean obtenidos del afectado el responsable del tratamiento podrá dar cumplimiento al deber de información establecido en el artículo 13 del Reglamento (UE) 2016/679 facilitando al afectado la información básica a la que se refiere el apartado siguiente e indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

2. La información básica a la que se refiere el apartado anterior deberá contener, al menos:

a) La identidad del responsable del tratamiento y de su representante, en su caso.
b) La finalidad del tratamiento.
c) La posibilidad de ejercer los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679.

Si los datos obtenidos del afectado fueran a ser tratados para la elaboración de perfiles, la información básica comprenderá asimismo esta circunstancia. En este caso, el afectado deberá ser informado de su derecho a oponerse a la adopción de decisiones individuales automatizadas que produzcan efectos jurídicos sobre él o le afecten significativamente de modo similar, cuando concurra este derecho de acuerdo con lo previsto en el artículo 22 del Reglamento (UE) 2016/679.

3. Cuando los datos personales no hubieran sido obtenidos del afectado, el responsable podrá dar cumplimiento al deber de información establecido en el artículo 14 del Reglamento (UE) 2016/679 facilitando a aquel la información básica señalada en el apartado anterior, indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

En estos supuestos, la información básica incluirá también:

a) Las categorías de datos objeto de tratamiento.
b) Las fuentes de las que procedieran los datos.

CAPÍTULO II

Ejercicio de los derechos

Artículo 12. *Disposiciones generales sobre ejercicio de los derechos.*

1. Los derechos reconocidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, podrán ejercerse directamente o por medio de representante legal o voluntario.

2. El responsable del tratamiento estará obligado a informar al afectado sobre los medios a su disposición para ejercer los derechos que le corresponden. Los medios deberán ser fácilmente accesibles para el afectado. El ejercicio del derecho no podrá ser denegado por el solo motivo de optar el afectado por otro medio.

3. El encargado podrá tramitar, por cuenta del responsable, las solicitudes de ejercicio formuladas por los afectados de sus derechos si así se estableciere en el contrato o acto jurídico que les vincule.

4. La prueba del cumplimiento del deber de responder a la solicitud de ejercicio de sus derechos formulado por el afectado recaerá sobre el responsable.

5. Cuando las leyes aplicables a determinados tratamientos establezcan un régimen especial que afecte al ejercicio de los derechos previstos en el Capítulo III del Reglamento (UE) 2016/679, se estará a lo dispuesto en aquellas.

6. En cualquier caso, los titulares de la patria potestad podrán ejercitar en nombre y representación de los menores de catorce años los derechos de acceso, rectificación, cancelación, oposición o cualesquiera otros que pudieran corresponderles en el contexto de la presente ley orgánica.

7. Serán gratuitas las actuaciones llevadas a cabo por el responsable del tratamiento para atender las solicitudes de ejercicio de estos derechos, sin perjuicio de lo dispuesto en los artículos 12.5 y 15.3 del Reglamento (UE) 2016/679 y en los apartados 3 y 4 del artículo 13 de esta ley orgánica.

Artículo 13. *Derecho de acceso.*

1. El derecho de acceso del afectado se ejercitará de acuerdo con lo establecido en el artículo 15 del Reglamento (UE) 2016/679.

Cuando el responsable trate una gran cantidad de datos relativos al afectado y este ejercite su derecho de acceso sin especificar si se refiere a todos o a una parte de los datos, el responsable podrá solicitarle, antes de facilitar la información, que el afectado especifique los datos o actividades de tratamiento a los que se refiere la solicitud.

2. El derecho de acceso se entenderá otorgado si el responsable del tratamiento facilitara al afectado un sistema de acceso remoto, directo y seguro a los datos personales

que garantice, de modo permanente, el acceso a su totalidad. A tales efectos, la comunicación por el responsable al afectado del modo en que este podrá acceder a dicho sistema bastará para tener por atendida la solicitud de ejercicio del derecho.

No obstante, el interesado podrá solicitar del responsable la información referida a los extremos previstos en el artículo 15.1 del Reglamento (UE) 2016/679 que no se incluyese en el sistema de acceso remoto.

3. A los efectos establecidos en el artículo 12.5 del Reglamento (UE) 2016/679 se podrá considerar repetitivo el ejercicio del derecho de acceso en más de una ocasión durante el plazo de seis meses, a menos que exista causa legítima para ello.

4. Cuando el afectado elija un medio distinto al que se le ofrece que suponga un coste desproporcionado, la solicitud será considerada excesiva, por lo que dicho afectado asumirá el exceso de costes que su elección comporte. En este caso, solo será exigible al responsable del tratamiento la satisfacción del derecho de acceso sin dilaciones indebidas.

Artículo 14. *Derecho de rectificación.*

Al ejercer el derecho de rectificación reconocido en el artículo 16 del Reglamento (UE) 2016/679, el afectado deberá indicar en su solicitud a qué datos se refiere y la corrección que haya de realizarse. Deberá acompañar, cuando sea preciso, la documentación justificativa de la inexactitud o carácter incompleto de los datos objeto de tratamiento.

Artículo 15. *Derecho de supresión.*

1. El derecho de supresión se ejercerá de acuerdo con lo establecido en el artículo 17 del Reglamento (UE) 2016/679.

2. Cuando la supresión derive del ejercicio del derecho de oposición con arreglo al artículo 21.2 del Reglamento (UE) 2016/679, el responsable podrá conservar los datos identificativos del afectado necesarios con el fin de impedir tratamientos futuros para fines de mercadotecnia directa.

Artículo 16. *Derecho a la limitación del tratamiento.*

1. El derecho a la limitación del tratamiento se ejercerá de acuerdo con lo establecido en el artículo 18 del Reglamento (UE) 2016/679.

2. El hecho de que el tratamiento de los datos personales esté limitado debe constar claramente en los sistemas de información del responsable.

Artículo 17. *Derecho a la portabilidad.*

El derecho a la portabilidad se ejercerá de acuerdo con lo establecido en el artículo 20 del Reglamento (UE) 2016/679.

Artículo 18. *Derecho de oposición.*

El derecho de oposición, así como los derechos relacionados con las decisiones individuales automatizadas, incluida la realización de perfiles, se ejercerán de acuerdo con lo establecido, respectivamente, en los artículos 21 y 22 del Reglamento (UE) 2016/679.

TÍTULO IV

Disposiciones aplicables a tratamientos concretos

Artículo 19. *Tratamiento de datos de contacto, de empresarios individuales y de profesionales liberales.*

1. Salvo prueba en contrario, se presumirá amparado en lo dispuesto en el artículo 6.1.f) del Reglamento (UE) 2016/679 el tratamiento de los datos de contacto y en su caso los relativos a la función o puesto desempeñado de las personas físicas que presten servicios en una persona jurídica siempre que se cumplan los siguientes requisitos:

a) Que el tratamiento se refiera únicamente a los datos necesarios para su localización profesional.

b) Que la finalidad del tratamiento sea únicamente mantener relaciones de cualquier índole con la persona jurídica en la que el afectado preste sus servicios.

2. La misma presunción operará para el tratamiento de los datos relativos a los empresarios individuales y a los profesionales liberales, cuando se refieran a ellos únicamente en dicha condición y no se traten para entablar una relación con los mismos como personas físicas.

3. Los responsables o encargados del tratamiento a los que se refiere el artículo 77.1 de esta ley orgánica podrán también tratar los datos mencionados en los dos apartados anteriores cuando ello se derive de una obligación legal o sea necesario para el ejercicio de sus competencias.

Artículo 20. *Sistemas de información crediticia.*

1. Salvo prueba en contrario, se presumirá lícito el tratamiento de datos personales relativos al incumplimiento de obligaciones dinerarias, financieras o de crédito por sistemas comunes de información crediticia cuando se cumplan los siguientes requisitos:

a) Que los datos hayan sido facilitados por el acreedor o por quien actúe por su cuenta o interés.

b) Que los datos se refieran a deudas ciertas, vencidas y exigibles, cuya existencia o cuantía no hubiese sido objeto de reclamación administrativa o judicial por el deudor o mediante un procedimiento alternativo de resolución de disputas vinculante entre las partes.

c) Que el acreedor haya informado al afectado en el contrato o en el momento de requerir el pago acerca de la posibilidad de inclusión en dichos sistemas, con indicación de aquéllos en los que participe.

La entidad que mantenga el sistema de información crediticia con datos relativos al incumplimiento de obligaciones dinerarias, financieras o de crédito deberá notificar al afectado la inclusión de tales datos y le informará sobre la posibilidad de ejercitar los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679 dentro de los treinta días siguientes a la notificación de la deuda al sistema, permaneciendo bloqueados los datos durante ese plazo.

d) Que los datos únicamente se mantengan en el sistema mientras persista el incumplimiento, con el límite máximo de cinco años desde la fecha de vencimiento de la obligación dineraria, financiera o de crédito.

e) Que los datos referidos a un deudor determinado solamente puedan ser consultados cuando quien consulte el sistema mantuviese una relación contractual con el afectado que implique el abono de una cuantía pecuniaria o este le hubiera solicitado la celebración de un contrato que suponga financiación, pago aplazado o facturación periódica, como sucede, entre otros supuestos, en los previstos en la legislación de contratos de crédito al consumo y de contratos de crédito inmobiliario.

Cuando se hubiera ejercitado ante el sistema el derecho a la limitación del tratamiento de los datos impugnando su exactitud conforme a lo previsto en el artículo 18.1.a) del Reglamento (UE) 2016/679, el sistema informará a quienes pudieran consultarlo con arreglo al párrafo anterior acerca de la mera existencia de dicha circunstancia, sin facilitar los datos concretos respecto de los que se hubiera ejercitado el derecho, en tanto se resuelve sobre la solicitud del afectado.

f) Que, en el caso de que se denegase la solicitud de celebración del contrato, o éste no llegara a celebrarse, como consecuencia de la consulta efectuada, quien haya consultado el sistema informe al afectado del resultado de dicha consulta.

2. Las entidades que mantengan el sistema y las acreedoras, respecto del tratamiento de los datos referidos a sus deudores, tendrán la condición de corresponsables del tratamiento de los datos, siendo de aplicación lo establecido por el artículo 26 del Reglamento (UE) 2016/679.

Corresponderá al acreedor garantizar que concurren los requisitos exigidos para la inclusión en el sistema de la deuda, respondiendo de su inexistencia o inexactitud.

3. La presunción a la que se refiere el apartado 1 de este artículo no ampara los supuestos en que la información crediticia fuese asociada por la entidad que mantuviera el sistema a informaciones adicionales a las contempladas en dicho apartado, relacionadas con el deudor y obtenidas de otras fuentes, a fin de llevar a cabo un perfilado del mismo, en particular mediante la aplicación de técnicas de calificación crediticia.

Artículo 21. *Tratamientos relacionados con la realización de determinadas operaciones mercantiles.*

1. Salvo prueba en contrario, se presumirán lícitos los tratamientos de datos, incluida su comunicación con carácter previo, que pudieran derivarse del desarrollo de cualquier operación de modificación estructural de sociedades o la aportación o transmisión de negocio o de rama de actividad empresarial, siempre que los tratamientos fueran necesarios para el buen fin de la operación y garanticen, cuando proceda, la continuidad en la prestación de los servicios.

2. En el caso de que la operación no llegara a concluirse, la entidad cesionaria deberá proceder con carácter inmediato a la supresión de los datos, sin que sea de aplicación la obligación de bloqueo prevista en esta ley orgánica.

Artículo 22. *Tratamientos con fines de videovigilancia.*

1. Las personas físicas o jurídicas, públicas o privadas, podrán llevar a cabo el tratamiento de imágenes a través de sistemas de cámaras o videocámaras con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones.

2. Solo podrán captarse imágenes de la vía pública en la medida en que resulte imprescindible para la finalidad mencionada en el apartado anterior.

No obstante, será posible la captación de la vía pública en una extensión superior cuando fuese necesario para garantizar la seguridad de bienes o instalaciones estratégicos o de infraestructuras vinculadas al transporte, sin que en ningún caso pueda suponer la captación de imágenes del interior de un domicilio privado.

3. Los datos serán suprimidos en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones. En tal caso, las imágenes deberán ser puestas a disposición de la autoridad competente en un plazo máximo de setenta y dos horas desde que se tuviera conocimiento de la existencia de la grabación.

No será de aplicación a estos tratamientos la obligación de bloqueo prevista en el artículo 32 de esta ley orgánica.

4. El deber de información previsto en el artículo 12 del Reglamento (UE) 2016/679 se entenderá cumplido mediante la colocación de un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679. También podrá incluirse en el dispositivo informativo un código de conexión o dirección de internet a esta información.

En todo caso, el responsable del tratamiento deberá mantener a disposición de los afectados la información a la que se refiere el citado reglamento.

5. Al amparo del artículo 2.2.c) del Reglamento (UE) 2016/679, se considera excluido de su ámbito de aplicación el tratamiento por una persona física de imágenes que solamente capten el interior de su propio domicilio.

Esta exclusión no abarca el tratamiento realizado por una entidad de seguridad privada que hubiera sido contratada para la vigilancia de un domicilio y tuviese acceso a las imágenes.

6. El tratamiento de los datos personales procedentes de las imágenes y sonidos obtenidos mediante la utilización de cámaras y videocámaras por las Fuerzas y Cuerpos de Seguridad y por los órganos competentes para la vigilancia y control en los centros penitenciarios y para el control, regulación, vigilancia y disciplina del tráfico, se regirá por la legislación de transposición de la Directiva (UE) 2016/680, cuando el tratamiento tenga fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública. Fuera de estos supuestos, dicho tratamiento se regirá

por su legislación específica y supletoriamente por el Reglamento (UE) 2016/679 y la presente ley orgánica.

7. Lo regulado en el presente artículo se entiende sin perjuicio de lo previsto en la Ley 5/2014, de 4 de abril, de Seguridad Privada y sus disposiciones de desarrollo.

8. El tratamiento por el empleador de datos obtenidos a través de sistemas de cámaras o videocámaras se somete a lo dispuesto en el artículo 89 de esta ley orgánica.

Artículo 23. *Sistemas de exclusión publicitaria.*

1. Será lícito el tratamiento de datos personales que tenga por objeto evitar el envío de comunicaciones comerciales a quienes hubiesen manifestado su negativa u oposición a recibirlas.

A tal efecto, podrán crearse sistemas de información, generales o sectoriales, en los que solo se incluirán los datos imprescindibles para identificar a los afectados. Estos sistemas también podrán incluir servicios de preferencia, mediante los cuales los afectados limiten la recepción de comunicaciones comerciales a las procedentes de determinadas empresas.

2. Las entidades responsables de los sistemas de exclusión publicitaria comunicarán a la autoridad de control competente su creación, su carácter general o sectorial, así como el modo en que los afectados pueden incorporarse a los mismos y, en su caso, hacer valer sus preferencias.

La autoridad de control competente hará pública en su sede electrónica una relación de los sistemas de esta naturaleza que le fueran comunicados, incorporando la información mencionada en el párrafo anterior. A tal efecto, la autoridad de control competente a la que se haya comunicado la creación del sistema lo pondrá en conocimiento de las restantes autoridades de control para su publicación por todas ellas.

3. Cuando un afectado manifieste a un responsable su deseo de que sus datos no sean tratados para la remisión de comunicaciones comerciales, este deberá informarle de los sistemas de exclusión publicitaria existentes, pudiendo remitirse a la información publicada por la autoridad de control competente.

4. Quienes pretendan realizar comunicaciones de mercadotecnia directa, deberán previamente consultar los sistemas de exclusión publicitaria que pudieran afectar a su actuación, excluyendo del tratamiento los datos de los afectados que hubieran manifestado su oposición o negativa al mismo. A estos efectos, para considerar cumplida la obligación anterior será suficiente la consulta de los sistemas de exclusión incluidos en la relación publicada por la autoridad de control competente.

No será necesario realizar la consulta a la que se refiere el párrafo anterior cuando el afectado hubiera prestado, conforme a lo dispuesto en esta ley orgánica, su consentimiento para recibir la comunicación a quien pretenda realizarla.

Artículo 24. *Tratamiento de datos para la protección de las personas que informen sobre infracciones normativas.*

Serán lícitos los tratamientos de datos personales necesarios para garantizar la protección de las personas que informen sobre infracciones normativas.

Dichos tratamientos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en esta ley orgánica y en la Ley reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.

Artículo 25. *Tratamiento de datos en el ámbito de la función estadística pública.*

1. El tratamiento de datos personales llevado a cabo por los organismos que tengan atribuidas las competencias relacionadas con el ejercicio de la función estadística pública se someterá a lo dispuesto en su legislación específica, así como en el Reglamento (UE) 2016/679 y en la presente ley orgánica.

2. La comunicación de los datos a los órganos competentes en materia estadística solo se entenderá amparada en el artículo 6.1 e) del Reglamento (UE) 2016/679 en los casos en que la estadística para la que se requiera la información venga exigida por una norma de

Derecho de la Unión Europea o se encuentre incluida en los instrumentos de programación estadística legalmente previstos.

De conformidad con lo dispuesto en el artículo 11.2 de la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública, serán de aportación estrictamente voluntaria y, en consecuencia, solo podrán recogerse previo consentimiento expreso de los afectados los datos a los que se refieren los artículos 9 y 10 del Reglamento (UE) 2016/679.

3. Los organismos competentes para el ejercicio de la función estadística pública podrán denegar las solicitudes de ejercicio por los afectados de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679 cuando los datos se encuentren amparados por las garantías del secreto estadístico previstas en la legislación estatal o autonómica.

Artículo 26. *Tratamiento de datos con fines de archivo en interés público por parte de las Administraciones Públicas.*

Será lícito el tratamiento por las Administraciones Públicas de datos con fines de archivo en interés público, que se someterá a lo dispuesto en el Reglamento (UE) 2016/679 y en la presente ley orgánica con las especialidades que se derivan de lo previsto en la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español, en el Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso, así como la legislación autonómica que resulte de aplicación.

Artículo 27. *Tratamiento de datos relativos a infracciones y sanciones administrativas.*

1. A los efectos del artículo 86 del Reglamento (UE) 2016/679, el tratamiento de datos relativos a infracciones y sanciones administrativas, incluido el mantenimiento de registros relacionados con las mismas, exigirá:

a) Que los responsables de dichos tratamientos sean los órganos competentes para la instrucción del procedimiento sancionador, para la declaración de las infracciones o la imposición de las sanciones.

b) Que el tratamiento se limite a los datos estrictamente necesarios para la finalidad perseguida por aquel.

2. Cuando no se cumpla alguna de las condiciones previstas en el apartado anterior, los tratamientos de datos referidos a infracciones y sanciones administrativas habrán de contar con el consentimiento del interesado o estar autorizados por una norma con rango de ley, en la que se regularán, en su caso, garantías adicionales para los derechos y libertades de los afectados.

3. Fuera de los supuestos señalados en los apartados anteriores, los tratamientos de datos referidos a infracciones y sanciones administrativas solo serán posibles cuando sean llevados a cabo por abogados y procuradores y tengan por objeto recoger la información facilitada por sus clientes para el ejercicio de sus funciones.

TÍTULO V

Responsable y encargado del tratamiento

CAPÍTULO I

Disposiciones generales. Medidas de responsabilidad activa

Artículo 28. *Obligaciones generales del responsable y encargado del tratamiento.*

1. Los responsables y encargados, teniendo en cuenta los elementos enumerados en los artículos 24 y 25 del Reglamento (UE) 2016/679, determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con el citado reglamento, con la presente ley orgánica, sus normas de desarrollo y la legislación sectorial aplicable. En particular valorarán si procede la realización

de la evaluación de impacto en la protección de datos y la consulta previa a que se refiere la Sección 3 del Capítulo IV del citado reglamento.

2. Para la adopción de las medidas a que se refiere el apartado anterior los responsables y encargados del tratamiento tendrán en cuenta, en particular, los mayores riesgos que podrían producirse en los siguientes supuestos:

a) Cuando el tratamiento pudiera generar situaciones de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados.

b) Cuando el tratamiento pudiese privar a los afectados de sus derechos y libertades o pudiera impedirles el ejercicio del control sobre sus datos personales.

c) Cuando se produjese el tratamiento no meramente incidental o accesorio de las categorías especiales de datos a las que se refieren los artículos 9 y 10 del Reglamento (UE) 2016/679 y 9 y 10 de esta ley orgánica o de los datos relacionados con la comisión de infracciones administrativas.

d) Cuando el tratamiento implicase una evaluación de aspectos personales de los afectados con el fin de crear o utilizar perfiles personales de los mismos, en particular mediante el análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, su situación económica, su salud, sus preferencias o intereses personales, su fiabilidad o comportamiento, su solvencia financiera, su localización o sus movimientos.

e) Cuando se lleve a cabo el tratamiento de datos de grupos de afectados en situación de especial vulnerabilidad y, en particular, de menores de edad y personas con discapacidad.

f) Cuando se produzca un tratamiento masivo que implique a un gran número de afectados o conlleve la recogida de una gran cantidad de datos personales.

g) Cuando los datos personales fuesen a ser objeto de transferencia, con carácter habitual, a terceros Estados u organizaciones internacionales respecto de los que no se hubiese declarado un nivel adecuado de protección.

h) Cualesquiera otros que a juicio del responsable o del encargado pudieran tener relevancia y en particular aquellos previstos en códigos de conducta y estándares definidos por esquemas de certificación.

Artículo 29. *Supuestos de corresponsabilidad en el tratamiento.*

La determinación de las responsabilidades a las que se refiere el artículo 26.1 del Reglamento (UE) 2016/679 se realizará atendiendo a las actividades que efectivamente desarrolle cada uno de los corresponsables del tratamiento.

Artículo 30. *Representantes de los responsables o encargados del tratamiento no establecidos en la Unión Europea.*

1. En los supuestos en que el Reglamento (UE) 2016/679 sea aplicable a un responsable o encargado del tratamiento no establecido en la Unión Europea en virtud de lo dispuesto en su artículo 3.2 y el tratamiento se refiera a afectados que se hallen en España, la Agencia Española de Protección de Datos o, en su caso, las autoridades autonómicas de protección de datos podrán imponer al representante, solidariamente con el responsable o encargado del tratamiento, las medidas establecidas en el Reglamento (UE) 2016/679.

Dicha exigencia se entenderá sin perjuicio de la responsabilidad que pudiera en su caso corresponder al responsable o al encargado del tratamiento y del ejercicio por el representante de la acción de repetición frente a quien proceda.

2. Asimismo, en caso de exigencia de responsabilidad en los términos previstos en el artículo 82 del Reglamento (UE) 2016/679, los responsables, encargados y representantes responderán solidariamente de los daños y perjuicios causados.

Artículo 31. *Registro de las actividades de tratamiento.*

1. Los responsables y encargados del tratamiento o, en su caso, sus representantes deberán mantener el registro de actividades de tratamiento al que se refiere el artículo 30 del

Reglamento (UE) 2016/679, salvo que sea de aplicación la excepción prevista en su apartado 5.

El registro, que podrá organizarse en torno a conjuntos estructurados de datos, deberá especificar, según sus finalidades, las actividades de tratamiento llevadas a cabo y las demás circunstancias establecidas en el citado reglamento.

Cuando el responsable o el encargado del tratamiento hubieran designado un delegado de protección de datos deberán comunicarle cualquier adición, modificación o exclusión en el contenido del registro.

2. Los sujetos enumerados en el artículo 77.1 de esta ley orgánica harán público un inventario de sus actividades de tratamiento accesible por medios electrónicos en el que constará la información establecida en el artículo 30 del Reglamento (UE) 2016/679 y su base legal.

Artículo 32. *Bloqueo de los datos.*

1. El responsable del tratamiento estará obligado a bloquear los datos cuando proceda a su rectificación o supresión.

2. El bloqueo de los datos consiste en la identificación y reserva de los mismos, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, excepto para la puesta a disposición de los datos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de las mismas.

Transcurrido ese plazo deberá procederse a la destrucción de los datos.

3. Los datos bloqueados no podrán ser tratados para ninguna finalidad distinta de la señalada en el apartado anterior.

4. Cuando para el cumplimiento de esta obligación, la configuración del sistema de información no permita el bloqueo o se requiera una adaptación que implique un esfuerzo desproporcionado, se procederá a un copiado seguro de la información de modo que conste evidencia digital, o de otra naturaleza, que permita acreditar la autenticidad de la misma, la fecha del bloqueo y la no manipulación de los datos durante el mismo.

5. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos, dentro del ámbito de sus respectivas competencias, podrán fijar excepciones a la obligación de bloqueo establecida en este artículo, en los supuestos en que, atendida la naturaleza de los datos o el hecho de que se refieran a un número particularmente elevado de afectados, su mera conservación, incluso bloqueados, pudiera generar un riesgo elevado para los derechos de los afectados, así como en aquellos casos en los que la conservación de los datos bloqueados pudiera implicar un coste desproporcionado para el responsable del tratamiento.

CAPÍTULO II

Encargado del tratamiento

Artículo 33. *Encargado del tratamiento.*

1. El acceso por parte de un encargado de tratamiento a los datos personales que resulten necesarios para la prestación de un servicio al responsable no se considerará comunicación de datos siempre que se cumpla lo establecido en el Reglamento (UE) 2016/679, en la presente ley orgánica y en sus normas de desarrollo.

2. Tendrá la consideración de responsable del tratamiento y no la de encargado quien en su propio nombre y sin que conste que actúa por cuenta de otro, establezca relaciones con los afectados aun cuando exista un contrato o acto jurídico con el contenido fijado en el artículo 28.3 del Reglamento (UE) 2016/679. Esta previsión no será aplicable a los encargos de tratamiento efectuados en el marco de la legislación de contratación del sector público.

Tendrá asimismo la consideración de responsable del tratamiento quien figurando como encargado utilizase los datos para sus propias finalidades.

3. El responsable del tratamiento determinará si, cuando finalice la prestación de los servicios del encargado, los datos personales deben ser destruidos, devueltos al responsable o entregados, en su caso, a un nuevo encargado.

No procederá la destrucción de los datos cuando exista una previsión legal que obligue a su conservación, en cuyo caso deberán ser devueltos al responsable, que garantizará su conservación mientras tal obligación persista.

4. El encargado del tratamiento podrá conservar, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.

5. En el ámbito del sector público podrán atribuirse las competencias propias de un encargado del tratamiento a un determinado órgano de la Administración General del Estado, la Administración de las comunidades autónomas, las Entidades que integran la Administración Local o a los Organismos vinculados o dependientes de las mismas mediante la adopción de una norma reguladora de dichas competencias, que deberá incorporar el contenido exigido por el artículo 28.3 del Reglamento (UE) 2016/679.

CAPÍTULO III

Delegado de protección de datos

Artículo 34. *Designación de un delegado de protección de datos.*

1. Los responsables y encargados del tratamiento deberán designar un delegado de protección de datos en los supuestos previstos en el artículo 37.1 del Reglamento (UE) 2016/679 y, en todo caso, cuando se trate de las siguientes entidades:

a) Los colegios profesionales y sus consejos generales.

b) Los centros docentes que ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación, así como las Universidades públicas y privadas.

c) Las entidades que exploten redes y presten servicios de comunicaciones electrónicas conforme a lo dispuesto en su legislación específica, cuando traten habitual y sistemáticamente datos personales a gran escala.

d) Los prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de los usuarios del servicio.

e) Las entidades incluidas en el artículo 1 de la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito.

f) Los establecimientos financieros de crédito.

g) Las entidades aseguradoras y reaseguradoras.

h) Las empresas de servicios de inversión, reguladas por la legislación del Mercado de Valores.

i) Los distribuidores y comercializadores de energía eléctrica y los distribuidores y comercializadores de gas natural.

j) Las entidades responsables de ficheros comunes para la evaluación de la solvencia patrimonial y crédito o de los ficheros comunes para la gestión y prevención del fraude, incluyendo a los responsables de los ficheros regulados por la legislación de prevención del blanqueo de capitales y de la financiación del terrorismo.

k) Las entidades que desarrollen actividades de publicidad y prospección comercial, incluyendo las de investigación comercial y de mercados, cuando lleven a cabo tratamientos basados en las preferencias de los afectados o realicen actividades que impliquen la elaboración de perfiles de los mismos.

l) Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes.

Se exceptúan los profesionales de la salud que, aun estando legalmente obligados al mantenimiento de las historias clínicas de los pacientes, ejerzan su actividad a título individual.

m) Las entidades que tengan como uno de sus objetos la emisión de informes comerciales que puedan referirse a personas físicas.

n) Los operadores que desarrollen la actividad de juego a través de canales electrónicos, informáticos, telemáticos e interactivos, conforme a la normativa de regulación del juego.

ñ) Las empresas de seguridad privada.

o) Las federaciones deportivas cuando traten datos de menores de edad.

2. Los responsables o encargados del tratamiento no incluidos en el párrafo anterior podrán designar de manera voluntaria un delegado de protección de datos, que quedará sometido al régimen establecido en el Reglamento (UE) 2016/679 y en la presente ley orgánica.

3. Los responsables y encargados del tratamiento comunicarán en el plazo de diez días a la Agencia Española de Protección de Datos o, en su caso, a las autoridades autonómicas de protección de datos, las designaciones, nombramientos y ceses de los delegados de protección de datos tanto en los supuestos en que se encuentren obligadas a su designación como en el caso en que sea voluntaria.

4. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos mantendrán, en el ámbito de sus respectivas competencias, una lista actualizada de delegados de protección de datos que será accesible por medios electrónicos.

5. En el cumplimiento de las obligaciones de este artículo los responsables y encargados del tratamiento podrán establecer la dedicación completa o a tiempo parcial del delegado, entre otros criterios, en función del volumen de los tratamientos, la categoría especial de los datos tratados o de los riesgos para los derechos o libertades de los interesados.

Artículo 35. *Cualificación del delegado de protección de datos.*

El cumplimiento de los requisitos establecidos en el artículo 37.5 del Reglamento (UE) 2016/679 para la designación del delegado de protección de datos, sea persona física o jurídica, podrá demostrarse, entre otros medios, a través de mecanismos voluntarios de certificación que tendrán particularmente en cuenta la obtención de una titulación universitaria que acredite conocimientos especializados en el derecho y la práctica en materia de protección de datos.

Artículo 36. *Posición del delegado de protección de datos.*

1. El delegado de protección de datos actuará como interlocutor del responsable o encargado del tratamiento ante la Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos. El delegado podrá inspeccionar los procedimientos relacionados con el objeto de la presente ley orgánica y emitir recomendaciones en el ámbito de sus competencias.

2. Cuando se trate de una persona física integrada en la organización del responsable o encargado del tratamiento, el delegado de protección de datos no podrá ser removido ni sancionado por el responsable o el encargado por desempeñar sus funciones salvo que incurriera en dolo o negligencia grave en su ejercicio. Se garantizará la independencia del delegado de protección de datos dentro de la organización, debiendo evitarse cualquier conflicto de intereses.

3. En el ejercicio de sus funciones el delegado de protección de datos tendrá acceso a los datos personales y procesos de tratamiento, no pudiendo oponer a este acceso el responsable o el encargado del tratamiento la existencia de cualquier deber de confidencialidad o secreto, incluyendo el previsto en el artículo 5 de esta ley orgánica.

4. Cuando el delegado de protección de datos aprecie la existencia de una vulneración relevante en materia de protección de datos lo documentará y lo comunicará inmediatamente a los órganos de administración y dirección del responsable o el encargado del tratamiento.

Artículo 37. *Intervención del delegado de protección de datos en caso de reclamación ante las autoridades de protección de datos.*

1. Cuando el responsable o el encargado del tratamiento hubieran designado un delegado de protección de datos el afectado podrá, con carácter previo a la presentación de una reclamación contra aquéllos ante la Agencia Española de Protección de Datos o, en su

caso, ante las autoridades autonómicas de protección de datos, dirigirse al delegado de protección de datos de la entidad contra la que se reclame.

En este caso, el delegado de protección de datos comunicará al afectado la decisión que se hubiera adoptado en el plazo máximo de dos meses a contar desde la recepción de la reclamación.

2. Cuando el afectado presente una reclamación ante la Agencia Española de Protección de Datos o, en su caso, ante las autoridades autonómicas de protección de datos, aquellas podrán remitir la reclamación al delegado de protección de datos a fin de que este responda en el plazo de un mes.

Si transcurrido dicho plazo el delegado de protección de datos no hubiera comunicado a la autoridad de protección de datos competente la respuesta dada a la reclamación, dicha autoridad continuará el procedimiento con arreglo a lo establecido en el Título VIII de esta ley orgánica y en sus normas de desarrollo.

3. El procedimiento ante la Agencia Española de Protección de Datos será el establecido en el Título VIII de esta ley orgánica y en sus normas de desarrollo. Asimismo, las comunidades autónomas regularán el procedimiento correspondiente ante sus autoridades autonómicas de protección de datos.

CAPÍTULO IV

Códigos de conducta y certificación

Artículo 38. *Códigos de conducta.*

1. Los códigos de conducta regulados por la sección 5.ª del Capítulo IV del Reglamento (UE) 2016/679 serán vinculantes para quienes se adhieran a los mismos.

Dichos códigos podrán dotarse de mecanismos de resolución extrajudicial de conflictos.

2. Dichos códigos podrán promoverse, además de por las asociaciones y organismos a los que se refiere el artículo 40.2 del Reglamento (UE) 2016/679, por empresas o grupos de empresas así como por los responsables o encargados a los que se refiere el artículo 77.1 de esta ley orgánica.

Asimismo, podrán ser promovidos por los organismos o entidades que asuman las funciones de supervisión y resolución extrajudicial de conflictos a los que se refiere el artículo 41 del Reglamento (UE) 2016/679.

Los responsables o encargados del tratamiento que se adhieran al código de conducta se obligan a someter al organismo o entidad de supervisión las reclamaciones que les fueran formuladas por los afectados en relación con los tratamientos de datos incluidos en su ámbito de aplicación en caso de considerar que no procede atender a lo solicitado en la reclamación, sin perjuicio de lo dispuesto en el artículo 37 de esta ley orgánica. Además, sin menoscabo de las competencias atribuidas por el Reglamento (UE) 2016/679 a las autoridades de protección de datos, podrán voluntariamente y antes de llevar a cabo el tratamiento, someter al citado organismo o entidad de supervisión la verificación de la conformidad del mismo con las materias sujetas al código de conducta.

En caso de que el organismo o entidad de supervisión rechace o desestime la reclamación, o si el responsable o encargado del tratamiento no somete la reclamación a su decisión, el afectado podrá formularla ante la Agencia Española de Protección de Datos o, en su caso, las autoridades autonómicas de protección de datos.

La autoridad de protección de datos competente verificará que los organismos o entidades que promuevan los códigos de conducta han dotado a estos códigos de organismos de supervisión que reúnan los requisitos establecidos en el artículo 41.2 del Reglamento (UE) 2016/679.

3. Los códigos de conducta serán aprobados por la Agencia Española de Protección de Datos o, en su caso, por la autoridad autonómica de protección de datos competente.

4. La Agencia Española de Protección de Datos o, en su caso, las autoridades autonómicas de protección de datos someterán los proyectos de código al mecanismo de coherencia mencionado en el artículo 63 de Reglamento (UE) 2016/679 en los supuestos en que ello proceda según su artículo 40.7. El procedimiento quedará suspendido en tanto el

Comité Europeo de Protección de Datos no emita el dictamen al que se refieren los artículos 64.1.b) y 65.1.c) del citado reglamento.

Cuando sea una autoridad autonómica de protección de datos la que someta el proyecto de código al mecanismo de coherencia, se estará a lo dispuesto en el artículo 60 de esta ley orgánica.

5. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos mantendrán registros de los códigos de conducta aprobados por las mismas, que estarán interconectados entre sí y coordinados con el registro gestionado por el Comité Europeo de Protección de Datos conforme al artículo 40.11 del citado reglamento.

El registro será accesible a través de medios electrónicos.

6. Mediante real decreto se establecerán el contenido del registro y las especialidades del procedimiento de aprobación de los códigos de conducta.

Artículo 39. *Acreditación de instituciones de certificación.*

Sin perjuicio de las funciones y poderes de acreditación de la autoridad de control competente en virtud de los artículos 57 y 58 del Reglamento (UE) 2016/679, la acreditación de las instituciones de certificación a las que se refiere el artículo 43.1 del citado reglamento podrá ser llevada a cabo por la Entidad Nacional de Acreditación (ENAC), que comunicará a la Agencia Española de Protección de Datos y a las autoridades de protección de datos de las comunidades autónomas las concesiones, denegaciones o revocaciones de las acreditaciones, así como su motivación.

TÍTULO VI

Transferencias internacionales de datos

Artículo 40. *Régimen de las transferencias internacionales de datos.*

Las transferencias internacionales de datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica y sus normas de desarrollo aprobadas por el Gobierno, y en las circulares de la Agencia Española de Protección de Datos y de las autoridades autonómicas de protección de datos, en el ámbito de sus respectivas competencias.

En todo caso se aplicarán a los tratamientos en que consista la propia transferencia las disposiciones contenidas en dichas normas, en particular las que regulan los principios de protección de datos.

Artículo 41. *Supuestos de adopción por la Agencia Española de Protección de Datos.*

1. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos podrán adoptar, conforme a lo dispuesto en el artículo 46.2.c) del Reglamento (UE) 2016/679, cláusulas contractuales tipo para la realización de transferencias internacionales de datos, que se someterán previamente al dictamen del Comité Europeo de Protección de Datos previsto en el artículo 64 del citado reglamento.

2. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos podrán aprobar normas corporativas vinculantes de acuerdo con lo previsto en el artículo 47 del Reglamento (UE) 2016/679.

El procedimiento se iniciará a instancia de una entidad situada en España y tendrá una duración máxima de nueve meses. Quedará suspendido como consecuencia de la remisión del expediente al Comité Europeo de Protección de Datos para que emita el dictamen al que se refiere el artículo 64.1.f) del Reglamento (UE) 2016/679, y continuará tras su notificación a la Agencia Española de Protección de Datos o a la autoridad autonómica de protección de datos competente.

Artículo 42. *Supuestos sometidos a autorización previa de las autoridades de protección de datos.*

1. Las transferencias internacionales de datos a países u organizaciones internacionales que no cuenten con decisión de adecuación aprobada por la Comisión o que no se amparen en alguna de las garantías previstas en el artículo anterior y en el artículo 46.2 del Reglamento (UE) 2016/679, requerirán una previa autorización de la Agencia Española de Protección de Datos o, en su caso, autoridades autonómicas de protección de datos, que podrá otorgarse en los siguientes supuestos:

a) Cuando la transferencia pretenda fundamentarse en la aportación de garantías adecuadas con fundamento en cláusulas contractuales que no correspondan a las cláusulas tipo previstas en el artículo 46.2, letras c) y d), del Reglamento (UE) 2016/679.

b) Cuando la transferencia se lleve a cabo por alguno de los responsables o encargados a los que se refiere el artículo 77.1 de esta ley orgánica y se funde en disposiciones incorporadas a acuerdos internacionales no normativos con otras autoridades u organismos públicos de terceros Estados, que incorporen derechos efectivos y exigibles para los afectados, incluidos los memorandos de entendimiento.

El procedimiento tendrá una duración máxima de seis meses.

2. La autorización quedará sometida a la emisión por el Comité Europeo de Protección de Datos del dictamen al que se refieren los artículos 64.1.e), 64.1.f) y 65.1.c) del Reglamento (UE) 2016/679. La remisión del expediente al citado comité implicará la suspensión del procedimiento hasta que el dictamen sea notificado a la Agencia Española de Protección de Datos o, por conducto de la misma, a la autoridad de control competente, en su caso.

Artículo 43. *Supuestos sometidos a información previa a la autoridad de protección de datos competente.*

Los responsables del tratamiento deberán informar a la Agencia Española de Protección de Datos o, en su caso, a las autoridades autonómicas de protección de datos, de cualquier transferencia internacional de datos que pretendan llevar a cabo sobre la base de su necesidad para fines relacionados con intereses legítimos imperiosos perseguidos por aquéllos y la concurrencia del resto de los requisitos previstos en el último párrafo del artículo 49.1 del Reglamento (UE) 2016/679. Asimismo, informarán a los afectados de la transferencia y de los intereses legítimos imperiosos perseguidos.

Esta información deberá facilitarse con carácter previo a la realización de la transferencia.

Lo dispuesto en este artículo no será de aplicación a las actividades llevadas a cabo por las autoridades públicas en el ejercicio de sus poderes públicos, de acuerdo con el artículo 49.3 del Reglamento (UE) 2016/679.

TÍTULO VII

Autoridades de protección de datos

CAPÍTULO I

La Agencia Española de Protección de Datos

Sección 1.ª Disposiciones generales

Artículo 44. *Disposiciones generales.*

1. La Agencia Española de Protección de Datos es una autoridad administrativa independiente de ámbito estatal, de las previstas en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, con personalidad jurídica y plena capacidad pública y privada, que actúa con plena independencia de los poderes públicos en el ejercicio de sus funciones.

Su denominación oficial, de conformidad con lo establecido en el artículo 109.3 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, será «Agencia Española de Protección de Datos, Autoridad Administrativa Independiente».

Se relaciona con el Gobierno a través del Ministerio de Justicia.

2. La Agencia Española de Protección de Datos tendrá la condición de representante común de las autoridades de protección de datos del Reino de España en el Comité Europeo de Protección de Datos.

3. La Agencia Española de Protección de Datos, el Consejo General del Poder Judicial y en su caso, la Fiscalía General del Estado, colaborarán en aras del adecuado ejercicio de las respectivas competencias que la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, les atribuye en materia de protección de datos personales en el ámbito de la Administración de Justicia.

Artículo 45. *Régimen jurídico.*

1. La Agencia Española de Protección de Datos se rige por lo dispuesto en el Reglamento (UE) 2016/679, la presente ley orgánica y sus disposiciones de desarrollo.

Supletoriamente, en cuanto sea compatible con su plena independencia y sin perjuicio de lo previsto en el artículo 63.2 de esta ley orgánica, se regirá por las normas citadas en el artículo 110.1 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

2. El Gobierno, a propuesta de la Agencia Española de Protección de Datos, aprobará su Estatuto mediante real decreto.

Artículo 46. *Régimen económico presupuestario y de personal.*

1. La Agencia Española de Protección de Datos elaborará y aprobará su presupuesto y lo remitirá al Gobierno para que sea integrado, con independencia, en los Presupuestos Generales del Estado.

2. El régimen de modificaciones y de vinculación de los créditos de su presupuesto será el establecido en el Estatuto de la Agencia Española de Protección de Datos.

Corresponde a la Presidencia de la Agencia Española de Protección de Datos autorizar las modificaciones presupuestarias que impliquen hasta un tres por ciento de la cifra inicial de su presupuesto total de gastos, siempre que no se incrementen los créditos para gastos de personal. Las restantes modificaciones que no excedan de un cinco por ciento del presupuesto serán autorizadas por el Ministerio de Hacienda y, en los demás casos, por el Gobierno.

3. La Agencia Española de Protección de Datos contará para el cumplimiento de sus fines con las asignaciones que se establezcan con cargo a los Presupuestos Generales del Estado, los bienes y valores que constituyan su patrimonio y los ingresos, ordinarios y extraordinarios derivados del ejercicio de sus actividades, incluidos los derivados del ejercicio de las potestades establecidos en el artículo 58 del Reglamento (UE) 2016/679.

4. El resultado positivo de sus ingresos se destinará por la Agencia Española de Protección de Datos a la dotación de sus reservas con el fin de garantizar su plena independencia.

5. El personal al servicio de la Agencia Española de Protección de Datos será funcionario o laboral y se regirá por lo previsto en el texto refundido de la Ley del Estatuto Básico del Empleado Público, aprobado por Real Decreto Legislativo 5/2015, de 30 de octubre, y demás normativa reguladora de los funcionarios públicos y, en su caso, por la normativa laboral.

6. La Agencia Española de Protección Datos elaborará y aprobará su relación de puestos de trabajo, en el marco de los criterios establecidos por el Ministerio de Hacienda, respetando el límite de gasto de personal establecido en el presupuesto. En dicha relación de puestos de trabajo constarán, en todo caso, aquellos puestos que deban ser desempeñados en exclusiva por funcionarios públicos, por consistir en el ejercicio de las funciones que impliquen la participación directa o indirecta en el ejercicio de potestades públicas y la salvaguarda de los intereses generales del Estado y de las Administraciones Públicas.

7. Sin perjuicio de las competencias atribuidas al Tribunal de Cuentas, la gestión económico-financiera de la Agencia Española de Protección de Datos estará sometida al

control de la Intervención General de la Administración del Estado en los términos que establece la Ley 47/2003, de 26 de noviembre, General Presupuestaria.

Artículo 47. *Funciones y potestades de la Agencia Española de Protección de Datos.*

Corresponde a la Agencia Española de Protección de Datos supervisar la aplicación de esta ley orgánica y del Reglamento (UE) 2016/679 y, en particular, ejercer las funciones establecidas en el artículo 57 y las potestades previstas en el artículo 58 del mismo reglamento, en la presente ley orgánica y en sus disposiciones de desarrollo.

Asimismo, corresponde a la Agencia Española de Protección de Datos el desempeño de las funciones y potestades que le atribuyan otras leyes o normas de Derecho de la Unión Europea.

Artículo 48. *La Presidencia de la Agencia Española de Protección de Datos.*

1. La Presidencia de la Agencia Española de Protección de Datos la dirige, ostenta su representación y dicta sus resoluciones, circulares y directrices.

2. La Presidencia de la Agencia Española de Protección de Datos estará auxiliada por un Adjunto en el que podrá delegar sus funciones, a excepción de las relacionadas con los procedimientos regulados por el título VIII de esta ley orgánica, y que la sustituirá en el ejercicio de las mismas en los términos previstos en el Estatuto Orgánico de la Agencia Española de Protección de Datos.

Ambos ejercerán sus funciones con plena independencia y objetividad y no estarán sujetos a instrucción alguna en su desempeño. Les será aplicable la legislación reguladora del ejercicio del alto cargo de la Administración General del Estado.

En los supuestos de ausencia, vacante o enfermedad de la persona titular de la Presidencia o cuando concurran en ella alguno de los motivos de abstención o recusación previstos en el artículo 23 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, el ejercicio de las competencias relacionadas con los procedimientos regulados por el título VIII de esta ley orgánica serán asumidas por la persona titular del órgano directivo que desarrolle las funciones de inspección. En el supuesto de que cualquiera de las circunstancias mencionadas concurriera igualmente en dicha persona, el ejercicio de las competencias afectadas será asumido por las personas titulares de los órganos directivos con nivel de subdirección general, por el orden establecido en el Estatuto.

El ejercicio del resto de competencias será asumido por el Adjunto en los términos previstos en el Estatuto Orgánico de la Agencia Española de Protección de Datos y, en su defecto, por las personas titulares de los órganos directivos con nivel de subdirección general, por el orden establecido en el Estatuto.

3. La Presidencia de la Agencia Española de Protección de Datos y su Adjunto serán nombrados por el Gobierno, a propuesta del Ministerio de Justicia, entre personas de reconocida competencia profesional, en particular en materia de protección de datos.

Dos meses antes de producirse la expiración del mandato o, en el resto de las causas de cese, cuando se haya producido éste, el Ministerio de Justicia ordenará la publicación en el Boletín Oficial del Estado de la convocatoria pública de candidatos.

Previa evaluación del mérito, capacidad, competencia e idoneidad de los candidatos, el Gobierno remitirá al Congreso de los Diputados una propuesta de Presidencia y Adjunto acompañada de un informe justificativo que, tras la celebración de la preceptiva audiencia de los candidatos, deberá ser ratificada por la Comisión de Justicia en votación pública por mayoría de tres quintos de sus miembros en primera votación o, de no alcanzarse ésta, por mayoría absoluta en segunda votación, que se realizará inmediatamente después de la primera. En este último supuesto, los votos favorables deberán proceder de Diputados pertenecientes, al menos, a dos grupos parlamentarios diferentes.

4. La Presidencia y el Adjunto de la Agencia Española de Protección de Datos serán nombrados por el Consejo de Ministros mediante real decreto.

5. El mandato de la Presidencia y del Adjunto de la Agencia Española de Protección de Datos tiene una duración de cinco años y puede ser renovado para otro período de igual duración.

La Presidencia y el Adjunto solo cesarán antes de la expiración de su mandato, a petición propia o por separación acordada por el Consejo de Ministros, por:

a) Incumplimiento grave de sus obligaciones,
b) incapacidad sobrevenida para el ejercicio de su función,
c) incompatibilidad, o
d) condena firme por delito doloso.

En los supuestos previstos en las letras a), b) y c) será necesaria la ratificación de la separación por las mayorías parlamentarias previstas en el apartado 3 de este artículo.

6. Los actos y disposiciones dictados por la Presidencia de la Agencia Española de Protección de Datos ponen fin a la vía administrativa, siendo recurribles, directamente, ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional.

Artículo 49. *Consejo Consultivo de la Agencia Española de Protección de Datos.*

1. La Presidencia de la Agencia Española de Protección de Datos estará asesorada por un Consejo Consultivo compuesto por los siguientes miembros:

a) Un Diputado, propuesto por el Congreso de los Diputados.
b) Un Senador, propuesto por el Senado.
c) Un representante designado por el Consejo General del Poder Judicial.
d) Un representante de la Administración General del Estado con experiencia en la materia, propuesto por el Ministro de Justicia.
e) Un representante de cada Comunidad Autónoma que haya creado una Autoridad de protección de datos en su ámbito territorial, propuesto de acuerdo con lo que establezca la respectiva Comunidad Autónoma.
f) Un experto propuesto por la Federación Española de Municipios y Provincias.
g) Un experto propuesto por el Consejo de Consumidores y Usuarios.
h) Dos expertos propuestos por las Organizaciones Empresariales.
i) Un representante de los profesionales de la protección de datos y de la privacidad, propuesto por la asociación de ámbito estatal con mayor número de asociados.
j) Un representante de los organismos o entidades de supervisión y resolución extrajudicial de conflictos previstos en el Capítulo IV del Título V, propuesto por el Ministro de Justicia.
k) Un experto, propuesto por la Conferencia de Rectores de las Universidades Españolas.
l) Un representante de las organizaciones que agrupan a los Consejos Generales, Superiores y Colegios Profesionales de ámbito estatal de las diferentes profesiones colegiadas, propuesto por el Ministro de Justicia.
m) Un representante de los profesionales de la seguridad de la información, propuesto por la asociación de ámbito estatal con mayor número de asociados.
n) Un experto en transparencia y acceso a la información pública propuesto por el Consejo de Transparencia y Buen Gobierno.
ñ) Dos expertos propuestos por las organizaciones sindicales más representativas.

2. A los efectos del apartado anterior, la condición de experto requerirá acreditar conocimientos especializados en el Derecho y la práctica en materia de protección de datos mediante el ejercicio profesional o académico.

3. Los miembros del Consejo Consultivo serán nombrados por orden del Ministro de Justicia, publicada en el Boletín Oficial del Estado.

4. El Consejo Consultivo se reunirá cuando así lo disponga la Presidencia de la Agencia Española de Protección de Datos y, en todo caso, una vez al semestre.

5. Las decisiones tomadas por el Consejo Consultivo no tendrán en ningún caso carácter vinculante.

6. En todo lo no previsto por esta ley orgánica, el régimen, competencias y funcionamiento del Consejo Consultivo serán los establecidos en el Estatuto Orgánico de la Agencia Española de Protección de Datos.

Artículo 50. *Publicidad.*

La Agencia Española de Protección de Datos publicará las resoluciones de su Presidencia que declaren haber lugar o no a la atención de los derechos reconocidos en los

artículos 15 a 22 del Reglamento (UE) 2016/679, las que pongan fin a los procedimientos sancionadores y a los procedimientos de apercibimiento, las que archiven las actuaciones previas de investigación, las dictadas respecto de las entidades a que se refiere el artículo 77.1 de esta ley orgánica, las que impongan medidas cautelares y las demás que disponga su Estatuto.

Sección 2.ª Potestades de investigación y planes de auditoría preventiva

Artículo 51. *Ámbito y personal competente.*

1. La Agencia Española de Protección de Datos desarrollará su actividad de investigación a través de las actuaciones previstas en el Título VIII y de los planes de auditoría preventivas.

2. La actividad de investigación se llevará a cabo por los funcionarios de la Agencia Española de Protección de Datos o por funcionarios ajenos a ella habilitados expresamente por su Presidencia.

3. En los casos de actuaciones conjuntas de investigación conforme a lo dispuesto en el artículo 62 del Reglamento (UE) 2016/679, el personal de las autoridades de control de otros Estados Miembros de Unión Europea que colabore con la Agencia Española de Protección de Datos ejercerá sus facultades con arreglo a lo previsto en la presente ley orgánica y bajo la orientación y en presencia del personal de esta.

4. Los funcionarios que desarrollen actividades de investigación tendrán la consideración de agentes de la autoridad en el ejercicio de sus funciones, y estarán obligados a guardar secreto sobre las informaciones que conozcan con ocasión de dicho ejercicio, incluso después de haber cesado en él.

Artículo 52. *Deber de colaboración.*

1. Las Administraciones Públicas, incluidas las tributarias y de la Seguridad Social, y los particulares estarán obligados a proporcionar a la Agencia Española de Protección de Datos los datos, informes, antecedentes y justificantes necesarios para llevar a cabo su actividad de investigación.

Cuando la información contenga datos personales la comunicación de dichos datos estará amparada por lo dispuesto en el artículo 6.1 c) del Reglamento (UE) 2016/679.

2. En el marco de las actuaciones previas de investigación, cuando no haya podido realizar la identificación por otros medios, la Agencia Española de Protección de Datos podrá recabar de las Administraciones Públicas, incluidas las tributarias y de la Seguridad Social, las informaciones y datos que resulten imprescindibles con la exclusiva finalidad de lograr la identificación de los responsables de las conductas que pudieran ser constitutivas de infracción del Reglamento (UE) 2016/679 y de la presente ley orgánica.

En el supuesto de las Administraciones tributarias y de la Seguridad Social, la información se limitará a la que resulte necesaria para poder identificar inequívocamente contra quién debe dirigirse la actuación de la Agencia Española de Protección de Datos en los supuestos de creación de entramados societarios que dificultasen el conocimiento directo del presunto responsable de la conducta contraria al Reglamento (UE) 2016/679 y a la presente ley orgánica.

3. Cuando no haya podido realizar la identificación por otros medios, la Agencia Española de Protección de Datos podrá recabar de los operadores que presten servicios de comunicaciones electrónicas disponibles al público y de los prestadores de servicios de la sociedad de la información los datos que obren en su poder y que resulten imprescindibles para la identificación del presunto responsable de la conducta contraria al Reglamento (UE) 2016/679 y a la presente ley orgánica cuando se hubiere llevado a cabo mediante la utilización de un servicio de la sociedad de la información o la realización de una comunicación electrónica. A tales efectos, los datos que la Agencia Española de Protección de Datos podrá recabar al amparo de este apartado son los siguientes:

a) Cuando la conducta se hubiera realizado mediante la utilización de un servicio de telefonía fija o móvil:

1.º El número de teléfono de origen de la llamada en caso de que el mismo se hubiese ocultado.

2.º El nombre, número de documento identificativo y dirección del abonado o usuario registrado al que corresponda ese número de teléfono.

3.º La mera confirmación de que se ha realizado una llamada específica entre dos números en una determinada fecha y hora.

b) Cuando la conducta se hubiera realizado mediante la utilización de un servicio de la sociedad de la información:

1.º La identificación de la dirección de protocolo de Internet desde la que se hubiera llevado a cabo la conducta y la fecha y hora de su realización.

2.º Si la conducta se hubiese llevado a cabo mediante correo electrónico, la identificación de la dirección de protocolo de Internet desde la que se creó la cuenta de correo y la fecha y hora en que la misma fue creada.

3.º El nombre, número de documento identificativo y dirección del abonado o del usuario registrado al que se le hubiera asignado la dirección de Protocolo de Internet a la que se refieren los dos párrafos anteriores.

Estos datos deberán ser cedidos, previo requerimiento motivado de la Agencia Española de Protección de Datos, exclusivamente en el marco de actuaciones de investigación iniciadas como consecuencia de una denuncia presentada por un afectado respecto de una conducta de una persona jurídica o respecto a la utilización de sistemas que permitan la divulgación sin restricciones de datos personales. En el resto de los supuestos la cesión de estos datos requerirá la previa obtención de autorización judicial otorgada conforme a las normas procesales cuando resultara exigible.

Quedan excluidos de lo previsto en este apartado los datos de tráfico que los operadores estuviesen tratando con la exclusiva finalidad de dar cumplimiento a las obligaciones previstas en la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, cuya cesión solamente podrá tener lugar de acuerdo con lo dispuesto en ella, previa autorización judicial solicitada por alguno de los agentes facultados a los que se refiere el artículo 6 de dicha ley.

Artículo 53. *Alcance de la actividad de investigación.*

1. Quienes desarrollen la actividad de investigación podrán recabar las informaciones precisas para el cumplimiento de sus funciones, realizar inspecciones, requerir la exhibición o el envío de los documentos y datos necesarios, examinarlos en el lugar en que se encuentren depositados o en donde se lleven a cabo los tratamientos, obtener copia de ellos, inspeccionar los equipos físicos y lógicos y requerir la ejecución de tratamientos y programas o procedimientos de gestión y soporte del tratamiento sujetos a investigación.

2. Cuando fuese necesario el acceso por el personal que desarrolla la actividad de investigación al domicilio constitucionalmente protegido del inspeccionado, será preciso contar con su consentimiento o haber obtenido la correspondiente autorización judicial.

3. Cuando se trate de órganos judiciales u oficinas judiciales el ejercicio de las facultades de inspección se efectuará a través y por mediación del Consejo General del Poder Judicial.

Artículo 53 bis. *Actuaciones de investigación a través de sistemas digitales.*

Las actuaciones de investigación podrán realizarse a través de sistemas digitales que, mediante la videoconferencia u otro sistema similar, permitan la comunicación bidireccional y simultánea de imagen y sonido, la interacción visual, auditiva y verbal entre la Agencia Española de Protección de Datos y el inspeccionado. Además, deben garantizar la transmisión y recepción seguras de los documentos e información que se intercambien, y, en su caso, recoger las evidencias necesarias y el resultado de las actuaciones realizadas asegurando su autoría, autenticidad e integridad.

La utilización de estos sistemas se producirá cuando lo determine la Agencia y requerirá la conformidad del inspeccionado en relación con su uso y con la fecha y hora de su desarrollo.

Artículo 54. *Planes de auditoría.*

1. La Presidencia de la Agencia Española de Protección de Datos podrá acordar la realización de planes de auditoría preventiva, referidos a los tratamientos de un sector concreto de actividad. Tendrán por objeto el análisis del cumplimiento de las disposiciones del Reglamento (UE) 2016/679 y de la presente ley orgánica, a partir de la realización de actividades de investigación sobre entidades pertenecientes al sector inspeccionado o sobre los responsables objeto de la auditoría.

2. A resultas de los planes de auditoría, la Presidencia de la Agencia Española de Protección de Datos podrá dictar las directrices generales o específicas para un concreto responsable o encargado de los tratamientos precisas para asegurar la plena adaptación del sector o responsable al Reglamento (UE) 2016/679 y a la presente ley orgánica.

En la elaboración de dichas directrices la Presidencia de la Agencia Española de Protección de Datos podrá solicitar la colaboración de los organismos de supervisión de los códigos de conducta y de resolución extrajudicial de conflictos, si los hubiere.

3. Las directrices serán de obligado cumplimiento para el sector o responsable al que se refiera el plan de auditoría.

Sección 3.ª Otras potestades de la Agencia Española de Protección de Datos

Artículo 55. *Potestades de regulación. Circulares de la Agencia Española de Protección de Datos.*

1. La Presidencia de la Agencia Española de Protección de Datos podrá dictar disposiciones que fijen los criterios a que responderá la actuación de esta autoridad en la aplicación de lo dispuesto en el Reglamento (UE) 2016/679 y en la presente ley orgánica, que se denominarán «Circulares de la Agencia Española de Protección de Datos».

2. Su elaboración se sujetará al procedimiento establecido en el Estatuto de la Agencia Española de Protección de Datos, que deberá prever los informes técnicos y jurídicos que fueran necesarios y la audiencia a los interesados.

3. Las circulares serán obligatorias una vez publicadas en el Boletín Oficial del Estado.

Artículo 56. *Acción exterior.*

1. Corresponde a la Agencia Española de Protección de Datos la titularidad y el ejercicio de las funciones relacionadas con la acción exterior del Estado en materia de protección de datos.

Asimismo a las comunidades autónomas, a través de las autoridades autonómicas de protección de datos, les compete ejercitar las funciones como sujetos de la acción exterior en el marco de sus competencias de conformidad con lo dispuesto en la Ley 2/2014, de 25 de marzo, de la Acción y del Servicio Exterior del Estado, así como celebrar acuerdos internacionales administrativos en ejecución y concreción de un tratado internacional y acuerdos no normativos con los órganos análogos de otros sujetos de derecho internacional, no vinculantes jurídicamente para quienes los suscriben, sobre materias de su competencia en el marco de la Ley 25/2014, de 27 de noviembre, de Tratados y otros Acuerdos Internacionales.

2. La Agencia Española de Protección de Datos es el organismo competente para la protección de las personas físicas en lo relativo al tratamiento de datos personales derivado de la aplicación de cualquier Convenio Internacional en el que sea parte el Reino de España que atribuya a una autoridad nacional de control esa competencia y la representante común de las autoridades de Protección de Datos en el Comité Europeo de Protección de Datos, conforme a lo dispuesto en el artículo 68.4 del Reglamento (UE) 2016/679.

La Agencia Española de Protección de Datos informará a las autoridades autonómicas de protección de datos acerca de las decisiones adoptadas en el Comité Europeo de Protección de Datos y recabará su parecer cuando se trate de materias de su competencia.

3. Sin perjuicio de lo dispuesto en el apartado 1, la Agencia Española de Protección de Datos:

a) Participará en reuniones y foros internacionales de ámbito distinto al de la Unión Europea establecidos de común acuerdo por las autoridades de control independientes en materia de protección de datos.

b) Participará, como autoridad española, en las organizaciones internacionales competentes en materia de protección de datos, en los comités o grupos de trabajo, de estudio y de colaboración de organizaciones internacionales que traten materias que afecten al derecho fundamental a la protección de datos personales y en otros foros o grupos de trabajo internacionales, en el marco de la acción exterior del Estado.

c) Colaborará con autoridades, instituciones, organismos y Administraciones de otros Estados a fin de impulsar, promover y desarrollar el derecho fundamental a la protección de datos, en particular en el ámbito iberoamericano, pudiendo suscribir acuerdos internacionales administrativos y no normativos en la materia.

CAPÍTULO II

Autoridades autonómicas de protección de datos

Sección 1.ª Disposiciones generales

Artículo 57. *Autoridades autonómicas de protección de datos.*

1. Las autoridades autonómicas de protección de datos personales podrán ejercer, las funciones y potestades establecidas en los artículos 57 y 58 del Reglamento (UE) 2016/679, de acuerdo con la normativa autonómica, cuando se refieran a:

a) Tratamientos de los que sean responsables las entidades integrantes del sector público de la correspondiente Comunidad Autónoma o de las Entidades Locales incluidas en su ámbito territorial o quienes presten servicios a través de cualquier forma de gestión directa o indirecta.

b) Tratamientos llevados a cabo por personas físicas o jurídicas para el ejercicio de las funciones públicas en materias que sean competencia de la correspondiente Administración Autonómica o Local.

c) Tratamientos que se encuentren expresamente previstos, en su caso, en los respectivos Estatutos de Autonomía.

2. Las autoridades autonómicas de protección de datos podrán dictar, en relación con los tratamientos sometidos a su competencia, circulares con el alcance y los efectos establecidos para la Agencia Española de Protección de Datos en el artículo 55 de esta ley orgánica.

Artículo 58. *Cooperación institucional.*

La Presidencia de la Agencia Española de Protección de Datos convocará, por iniciativa propia o cuando lo solicite otra autoridad, a las autoridades autonómicas de protección de datos para contribuir a la aplicación coherente del Reglamento (UE) 2016/679 y de la presente ley orgánica. En todo caso, se celebrarán reuniones semestrales de cooperación.

La Presidencia de la Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos podrán solicitar y deberán intercambiarse mutuamente la información necesaria para el cumplimiento de sus funciones y, en particular, la relativa a la actividad del Comité Europeo de Protección de Datos. Asimismo, podrán constituir grupos de trabajo para tratar asuntos específicos de interés común.

Artículo 59. *Tratamientos contrarios al Reglamento (UE) 2016/679.*

Cuando la Presidencia de la Agencia Española de Protección de Datos considere que un tratamiento llevado a cabo en materias que fueran competencia de las autoridades autonómicas de protección de datos vulnera el Reglamento (UE) 2016/679 podrá requerirlas a que adopten, en el plazo de un mes, las medidas necesarias para su cesación.

Si la autoridad autonómica no atendiere en plazo el requerimiento o las medidas adoptadas no supusiesen la cesación en el tratamiento ilícito, la Agencia Española de

Protección de Datos podrá ejercer las acciones que procedan ante la jurisdicción contencioso-administrativa.

Sección 2.ª Coordinación en el marco de los procedimientos establecidos en el Reglamento (UE) 2016/679

Artículo 60. *Coordinación en caso de emisión de dictamen por el Comité Europeo de Protección de Datos.*

Se practicarán por conducto de la Agencia Española de Protección de Datos todas las comunicaciones entre el Comité Europeo de Protección de Datos y las autoridades autonómicas de protección de datos cuando éstas, como autoridades competentes, deban someter su proyecto de decisión al citado comité o le soliciten el examen de un asunto en virtud de lo establecido en los apartados 1 y 2 del artículo 64 del Reglamento (UE) 2016/679.

En estos casos, la Agencia Española de Protección de Datos será asistida por un representante de la Autoridad autonómica en su intervención ante el Comité.

Artículo 61. *Intervención en caso de tratamientos transfronterizos.*

1. Las autoridades autonómicas de protección de datos ostentarán la condición de autoridad de control principal o interesada en el procedimiento establecido por el artículo 60 del Reglamento (UE) 2016/679 cuando se refiera a un tratamiento previsto en el artículo 57 de esta ley orgánica que se llevara a cabo por un responsable o encargado del tratamiento de los previstos en el artículo 56 del Reglamento (UE) 2016/679, salvo que desarrollase significativamente tratamientos de la misma naturaleza en el resto del territorio español.

2. Corresponderá en estos casos a las autoridades autonómicas intervenir en los procedimientos establecidos en el artículo 60 del Reglamento (UE) 2016/679, informando a la Agencia Española de Protección de Datos sobre su desarrollo en los supuestos en que deba aplicarse el mecanismo de coherencia.

Artículo 62. *Coordinación en caso de resolución de conflictos por el Comité Europeo de Protección de Datos.*

1. Se practicarán por conducto de la Agencia Española de Protección de Datos todas las comunicaciones entre el Comité Europeo de Protección de Datos y las autoridades autonómicas de protección de datos cuando estas, como autoridades principales, deban solicitar del citado Comité la emisión de una decisión vinculante según lo previsto en el artículo 65 del Reglamento (UE) 2016/679.

2. Las autoridades autonómicas de protección de datos que tengan la condición de autoridad interesada no principal en un procedimiento de los previstos en el artículo 65 del Reglamento (UE) 2016/679 informarán a la Agencia Española de Protección de Datos cuando el asunto sea remitido al Comité Europeo de Protección de Datos, facilitándole la documentación e información necesarias para su tramitación.

La Agencia Española de Protección de Datos será asistida por un representante de la autoridad autonómica interesada en su intervención ante el mencionado comité.

TÍTULO VIII

Procedimientos en caso de posible vulneración de la normativa de protección de datos

Artículo 63. *Régimen jurídico.*

1. Las disposiciones de este Título serán de aplicación a los procedimientos tramitados por la Agencia Española de Protección de Datos en los supuestos en los que un afectado reclame que no ha sido atendida su solicitud de ejercicio de los derechos reconocidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, así como en los que aquella investigue la existencia de una posible infracción de lo dispuesto en el mencionado reglamento y en la presente ley orgánica.

2. Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos.

3. El Gobierno regulará por real decreto los procedimientos que tramite la Agencia Española de Protección de Datos al amparo de este Título, asegurando en todo caso los derechos de defensa y audiencia de los interesados.

Artículo 64. *Forma de iniciación del procedimiento y duración.*

1. Cuando el procedimiento se refiera exclusivamente a la falta de atención de una solicitud de ejercicio de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, se iniciará por acuerdo de admisión a trámite, que se adoptará conforme a lo establecido en el artículo 65 de esta ley orgánica.

En este caso el plazo para resolver el procedimiento será de seis meses a contar desde la fecha en que hubiera sido notificado al reclamante el acuerdo de admisión a trámite. Transcurrido ese plazo, el interesado podrá considerar estimada su reclamación.

2. Cuando el procedimiento tenga por objeto la determinación de la posible existencia de una infracción de lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y en la presente ley orgánica, se iniciará mediante acuerdo de inicio, adoptado por propia iniciativa o como consecuencia de reclamación, que le será notificado al interesado.

Si el procedimiento se fundase en una reclamación formulada ante la Agencia Española de Protección de Datos, con carácter previo, esta decidirá sobre su admisión a trámite, conforme a lo dispuesto en el artículo 65 de esta ley orgánica.

Admitida a trámite la reclamación, así como en los supuestos en que la Agencia Española de Protección de Datos actúe por propia iniciativa, con carácter previo al acuerdo de inicio podrá existir una fase de actuaciones previas de investigación, que se regirá por lo previsto en el artículo 67 de esta ley orgánica.

El procedimiento tendrá una duración máxima de doce meses a contar desde la fecha del acuerdo de inicio. Transcurrido ese plazo se producirá su caducidad y, en consecuencia, el archivo de actuaciones.

3. Cuando así proceda en atención a la naturaleza de los hechos y teniendo debidamente en cuenta los criterios establecidos en el artículo 83.2 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, la Agencia Española de Protección de Datos, previa audiencia al responsable o encargado del tratamiento, podrá dirigir un apercibimiento, así como ordenar al responsable o encargado del tratamiento que adopten las medidas correctivas encaminadas a poner fin al posible incumplimiento de la legislación de protección de datos de una determinada manera y dentro del plazo especificado.

El procedimiento tendrá una duración máxima de seis meses a contar desde la fecha del acuerdo de inicio. Transcurrido ese plazo se producirá su caducidad y, en consecuencia, el archivo de actuaciones.

Será de aplicación en este caso lo dispuesto en los párrafos segundo y tercero del apartado 2 de este artículo.

4. El procedimiento podrá también tramitarse como consecuencia de la comunicación a la Agencia Española de Protección de Datos por parte de la autoridad de control de otro Estado miembro de la Unión Europea de la reclamación formulada ante la misma, cuando la Agencia Española de Protección de Datos tuviese la condición de autoridad de control principal para la tramitación de un procedimiento conforme a lo dispuesto en los artículos 56 y 60 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016. Será en este caso de aplicación lo dispuesto en los apartados 1, 2 y 3 de este artículo.

5. Los plazos de tramitación establecidos en este artículo así como los de admisión a trámite regulados por el artículo 65.5 y de duración de las actuaciones previas de investigación previstos en el artículo 67.2, quedarán automáticamente suspendidos cuando deba recabarse información, consulta, solicitud de asistencia o pronunciamiento preceptivo de un órgano u organismo de la Unión Europea o de una o varias autoridades de control de

los Estados miembros conforme con lo establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, por el tiempo que medie entre la solicitud y la notificación del pronunciamiento a la Agencia Española de Protección de Datos.

6. El transcurso de los plazos de tramitación a los que se refiere el apartado anterior se podrá suspender, mediante resolución motivada, cuando resulte indispensable recabar información de un órgano jurisdiccional.

Artículo 65. *Admisión a trámite de las reclamaciones.*

1. Cuando se presentase ante la Agencia Española de Protección de Datos una reclamación, esta deberá evaluar su admisibilidad a trámite, de conformidad con las previsiones de este artículo.

2. La Agencia Española de Protección de Datos inadmitirá las reclamaciones presentadas cuando no versen sobre cuestiones de protección de datos personales, carezcan manifiestamente de fundamento, sean abusivas o no aporten indicios racionales de la existencia de una infracción.

3. Igualmente, la Agencia Española de Protección de Datos podrá inadmitir la reclamación cuando el responsable o encargado del tratamiento, previa advertencia formulada por la Agencia Española de Protección de Datos, hubiera adoptado las medidas correctivas encaminadas a poner fin al posible incumplimiento de la legislación de protección de datos y concurra alguna de las siguientes circunstancias:

a) Que no se haya causado perjuicio al afectado en el caso de las infracciones previstas en el artículo 74 de esta ley orgánica.

b) Que el derecho del afectado quede plenamente garantizado mediante la aplicación de las medidas.

4. Antes de resolver sobre la admisión a trámite de la reclamación, la Agencia Española de Protección de Datos podrá remitir la misma al delegado de protección de datos que hubiera, en su caso, designado el responsable o encargado del tratamiento, al organismo de supervisión establecido para la aplicación de los códigos de conducta o al organismo que asuma las funciones de resolución extrajudicial de conflictos a los efectos previstos en los artículos 37 y 38.2 de esta ley orgánica.

La Agencia Española de Protección de Datos podrá igualmente remitir la reclamación al responsable o encargado del tratamiento cuando no se hubiera designado un delegado de protección de datos ni estuviera adherido a mecanismos de resolución extrajudicial de conflictos, en cuyo caso el responsable o encargado deberá dar respuesta a la reclamación en el plazo de un mes.

Si como consecuencia de dichas actuaciones de remisión, el responsable o encargado del tratamiento demuestra haber adoptado medidas para el cumplimiento de la normativa aplicable, la Agencia Española de Protección de Datos podrá inadmitir a trámite la reclamación.

5. La decisión sobre la admisión o inadmisión a trámite, así como la que determine, en su caso, la remisión de la reclamación a la autoridad de control principal que se estime competente, deberá notificarse al reclamante en el plazo de tres meses. Si transcurrido este plazo no se produjera dicha notificación, se entenderá que prosigue la tramitación de la reclamación con arreglo a lo dispuesto en este título a partir de la fecha en que se cumpliesen tres meses desde que la reclamación tuvo entrada en la Agencia Española de Protección de Datos, sin perjuicio de la facultad de la Agencia de archivar posteriormente y de forma expresa la reclamación.

En el supuesto de que la Agencia Española de Protección de Datos actúe como consecuencia de la comunicación que le hubiera sido remitida por la autoridad de control de otro Estado miembro de la Unión Europea, conforme al artículo 64.4 de esta ley orgánica, el cómputo del plazo señalado en el párrafo anterior se iniciará una vez que se reciba en la Agencia toda la documentación necesaria para su tramitación.

Cuando los hechos de una reclamación relativa a la posible existencia en el ámbito competencial de la Agencia, guarden identidad sustancial con los que sean objeto de unas actuaciones previas de investigación o de un procedimiento sancionador ya iniciado, en la notificación de la decisión de admisión a trámite se podrá indicar el número de expediente

correspondiente a las actuaciones previas o al procedimiento correspondiente, así como de la dirección web en la que se publicará la resolución que ponga fin al mismo, a efectos de que el reclamante pueda conocer el curso y resultado de la investigación.

6. Tras la admisión a trámite, si el responsable o encargado del tratamiento demuestran haber adoptado medidas para el cumplimiento de la normativa aplicable, la Agencia Española de Protección de Datos podrá resolver el archivo de la reclamación, cuando en el caso concreto concurran circunstancias que aconsejen la adopción de otras soluciones más moderadas o alternativas a la acción correctiva, siempre que no se hayan iniciado actuaciones previas de investigación o alguno de los procedimientos regulados en esta ley orgánica.

Artículo 66. *Determinación del alcance territorial.*

1. Salvo en los supuestos a los que se refiere el artículo 64.4 de esta ley orgánica, la Agencia Española de Protección de Datos deberá, con carácter previo a la realización de cualquier otra actuación, incluida la admisión a trámite de una reclamación o el comienzo de actuaciones previas de investigación, examinar su competencia y determinar el carácter nacional o transfronterizo, en cualquiera de sus modalidades, del procedimiento a seguir.

2. Si la Agencia Española de Protección de Datos considera que no tiene la condición de autoridad de control principal para la tramitación del procedimiento remitirá, sin más trámite, la reclamación formulada a la autoridad de control principal que considere competente, a fin de que por la misma se le dé el curso oportuno. La Agencia Española de Protección de Datos notificará esta circunstancia a quien, en su caso, hubiera formulado la reclamación.

El acuerdo por el que se resuelva la remisión a la que se refiere el párrafo anterior implicará el archivo provisional del procedimiento, sin perjuicio de que por la Agencia Española de Protección de Datos se dicte, en caso de que así proceda, la resolución a la que se refiere el apartado 8 del artículo 60 del Reglamento (UE) 2016/679.

Artículo 67. *Actuaciones previas de investigación.*

1. Antes de la adopción del acuerdo de inicio de procedimiento, y una vez admitida a trámite la reclamación si la hubiese, la Agencia Española de Protección de Datos podrá llevar a cabo actuaciones previas de investigación a fin de lograr una mejor determinación de los hechos y las circunstancias que justifican la tramitación del procedimiento.

La Agencia Española de Protección de Datos actuará en todo caso cuando sea precisa la investigación de tratamientos que implique un tráfico masivo de datos personales.

2. Las actuaciones previas de investigación se someterán a lo dispuesto en la sección 2.ª del capítulo I del título VII de esta ley orgánica y no podrán tener una duración superior a dieciocho meses a contar desde la fecha del acuerdo de admisión a trámite o de la fecha del acuerdo por el que se decida su iniciación cuando la Agencia Española de Protección de Datos actúe por propia iniciativa.

Artículo 68. *Acuerdo de inicio del procedimiento para el ejercicio de la potestad sancionadora.*

1. Concluidas, en su caso, las actuaciones a las que se refiere el artículo anterior, corresponderá a la Presidencia de la Agencia Española de Protección de Datos, cuando así proceda, dictar acuerdo de inicio de procedimiento para el ejercicio de la potestad sancionadora, en que se concretarán los hechos, la identificación de la persona o entidad contra la que se dirija el procedimiento, la infracción que hubiera podido cometerse y su posible sanción.

2. Cuando la Agencia Española de Protección de Datos ostente la condición de autoridad de control principal y deba seguirse el procedimiento previsto en el artículo 60 del Reglamento (UE) 2016/679, el proyecto de acuerdo de inicio de procedimiento sancionador se someterá a lo dispuesto en el mismo.

Artículo 69. *Medidas provisionales y de garantía de los derechos.*

1. Durante la realización de las actuaciones previas de investigación o iniciado un procedimiento para el ejercicio de la potestad sancionadora, la Agencia Española de

Protección de Datos podrá acordar motivadamente las medidas provisionales necesarias y proporcionadas para salvaguardar el derecho fundamental a la protección de datos y, en especial, las previstas en el artículo 66.1 del Reglamento (UE) 2016/679, el bloqueo cautelar de los datos y la obligación inmediata de atender el derecho solicitado.

2. En los casos en que la Agencia Española de Protección de Datos considere que la continuación del tratamiento de los datos personales, su comunicación o transferencia internacional comportara un menoscabo grave del derecho a la protección de datos personales, podrá ordenar a los responsables o encargados de los tratamientos el bloqueo de los datos y la cesación de su tratamiento y, en caso de incumplirse por estos dichos mandatos, proceder a su inmovilización.

3. Cuando se hubiese presentado ante la Agencia Española de Protección de Datos una reclamación que se refiriese, entre otras cuestiones, a la falta de atención en plazo de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, la Agencia Española de Protección de Datos podrá acordar en cualquier momento, incluso con anterioridad a la iniciación del procedimiento para el ejercicio de la potestad sancionadora, mediante resolución motivada y previa audiencia del responsable del tratamiento, la obligación de atender el derecho solicitado, prosiguiéndose el procedimiento en cuanto al resto de las cuestiones objeto de la reclamación.

TÍTULO IX

Régimen sancionador

Artículo 70. *Sujetos responsables.*

1. Están sujetos al régimen sancionador establecido en el Reglamento (UE) 2016/679 y en la presente ley orgánica:

a) Los responsables de los tratamientos.
b) Los encargados de los tratamientos.
c) Los representantes de los responsables o encargados de los tratamientos no establecidos en el territorio de la Unión Europea.
d) Las entidades de certificación.
e) Las entidades acreditadas de supervisión de los códigos de conducta.

2. No será de aplicación al delegado de protección de datos el régimen sancionador establecido en este Título.

Artículo 71. *Infracciones.*

Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica.

Artículo 72. *Infracciones consideradas muy graves.*

1. En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

a) El tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 5 del Reglamento (UE) 2016/679.
b) El tratamiento de datos personales sin que concurra alguna de las condiciones de licitud del tratamiento establecidas en el artículo 6 del Reglamento (UE) 2016/679.
c) El incumplimiento de los requisitos exigidos por el artículo 7 del Reglamento (UE) 2016/679 para la validez del consentimiento.
d) La utilización de los datos para una finalidad que no sea compatible con la finalidad para la cual fueron recogidos, sin contar con el consentimiento del afectado o con una base legal para ello.

e) El tratamiento de datos personales de las categorías a las que se refiere el artículo 9 del Reglamento (UE) 2016/679, sin que concurra alguna de las circunstancias previstas en dicho precepto y en el artículo 9 de esta ley orgánica.

f) El tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas fuera de los supuestos permitidos por el artículo 10 del Reglamento (UE) 2016/679 y en el artículo 10 de esta ley orgánica.

g) El tratamiento de datos personales relacionados con infracciones y sanciones administrativas fuera de los supuestos permitidos por el artículo 27 de esta ley orgánica.

h) La omisión del deber de informar al afectado acerca del tratamiento de sus datos personales conforme a lo dispuesto en los artículos 13 y 14 del Reglamento (UE) 2016/679 y 12 de esta ley orgánica.

i) La vulneración del deber de confidencialidad establecido en el artículo 5 de esta ley orgánica.

j) La exigencia del pago de un canon para facilitar al afectado la información a la que se refieren los artículos 13 y 14 del Reglamento (UE) 2016/679 o por atender las solicitudes de ejercicio de derechos de los afectados previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679, fuera de los supuestos establecidos en su artículo 12.5.

k) El impedimento o la obstaculización o la no atención reiterada del ejercicio de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679.

l) La transferencia internacional de datos personales a un destinatario que se encuentre en un tercer país o a una organización internacional, cuando no concurran las garantías, requisitos o excepciones establecidos en los artículos 44 a 49 del Reglamento (UE) 2016/679.

m) El incumplimiento de las resoluciones dictadas por la autoridad de protección de datos competente en ejercicio de los poderes que le confiere el artículo 58.2 del Reglamento (UE) 2016/679.

n) El incumplimiento de la obligación de bloqueo de los datos establecida en el artículo 32 de esta ley orgánica cuando la misma sea exigible.

ñ) No facilitar el acceso del personal de la autoridad de protección de datos competente a los datos personales, información, locales, equipos y medios de tratamiento que sean requeridos por la autoridad de protección de datos para el ejercicio de sus poderes de investigación.

o) La resistencia u obstrucción del ejercicio de la función inspectora por la autoridad de protección de datos competente.

p) La reversión deliberada de un procedimiento de anonimización a fin de permitir la reidentificación de los afectados.

2. Tendrán la misma consideración y también prescribirán a los tres años las infracciones a las que se refiere el artículo 83.6 del Reglamento (UE) 2016/679.

Artículo 73. *Infracciones consideradas graves.*

En función de lo que establece el artículo 83.4 del Reglamento (UE) 2016/679 se consideran graves y prescribirán a los dos años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

a) El tratamiento de datos personales de un menor de edad sin recabar su consentimiento, cuando tenga capacidad para ello, o el del titular de su patria potestad o tutela, conforme al artículo 8 del Reglamento (UE) 2016/679.

b) No acreditar la realización de esfuerzos razonables para verificar la validez del consentimiento prestado por un menor de edad o por el titular de su patria potestad o tutela sobre el mismo, conforme a lo requerido por el artículo 8.2 del Reglamento (UE) 2016/679.

c) El impedimento o la obstaculización o la no atención reiterada de los derechos de acceso, rectificación, supresión, limitación del tratamiento o a la portabilidad de los datos en tratamientos en los que no se requiere la identificación del afectado, cuando este, para el ejercicio de esos derechos, haya facilitado información adicional que permita su identificación.

d) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para aplicar de forma efectiva los principios de protección de datos desde el

diseño, así como la no integración de las garantías necesarias en el tratamiento, en los términos exigidos por el artículo 25 del Reglamento (UE) 2016/679.

e) La falta de adopción de las medidas técnicas y organizativas apropiadas para garantizar que, por defecto, solo se tratarán los datos personales necesarios para cada uno de los fines específicos del tratamiento, conforme a lo exigido por el artículo 25.2 del Reglamento (UE) 2016/679.

f) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679.

g) El quebrantamiento, como consecuencia de la falta de la debida diligencia, de las medidas técnicas y organizativas que se hubiesen implantado conforme a lo exigido por el artículo 32.1 del Reglamento (UE) 2016/679.

h) El incumplimiento de la obligación de designar un representante del responsable o encargado del tratamiento no establecido en el territorio de la Unión Europea, conforme a lo previsto en el artículo 27 del Reglamento (UE) 2016/679.

i) La falta de atención por el representante en la Unión del responsable o del encargado del tratamiento de las solicitudes efectuadas por la autoridad de protección de datos o por los afectados.

j) La contratación por el responsable del tratamiento de un encargado de tratamiento que no ofrezca las garantías suficientes para aplicar las medidas técnicas y organizativas apropiadas conforme a lo establecido en el Capítulo IV del Reglamento (UE) 2016/679.

k) Encargar el tratamiento de datos a un tercero sin la previa formalización de un contrato u otro acto jurídico escrito con el contenido exigido por el artículo 28.3 del Reglamento (UE) 2016/679.

l) La contratación por un encargado del tratamiento de otros encargados sin contar con la autorización previa del responsable, o sin haberle informado sobre los cambios producidos en la subcontratación cuando fueran legalmente exigibles.

m) La infracción por un encargado del tratamiento de lo dispuesto en el Reglamento (UE) 2016/679 y en la presente ley orgánica, al determinar los fines y los medios del tratamiento, conforme a lo dispuesto en el artículo 28.10 del citado reglamento.

n) No disponer del registro de actividades de tratamiento establecido en el artículo 30 del Reglamento (UE) 2016/679.

ñ) No poner a disposición de la autoridad de protección de datos que lo haya solicitado, el registro de actividades de tratamiento, conforme al apartado 4 del artículo 30 del Reglamento (UE) 2016/679.

o) No cooperar con las autoridades de control en el desempeño de sus funciones en los supuestos no previstos en el artículo 72 de esta ley orgánica.

p) El tratamiento de datos personales sin llevar a cabo una previa valoración de los elementos mencionados en el artículo 28 de esta ley orgánica.

q) El incumplimiento del deber del encargado del tratamiento de notificar al responsable del tratamiento las violaciones de seguridad de las que tuviera conocimiento.

r) El incumplimiento del deber de notificación a la autoridad de protección de datos de una violación de seguridad de los datos personales de conformidad con lo previsto en el artículo 33 del Reglamento (UE) 2016/679.

s) El incumplimiento del deber de comunicación al afectado de una violación de la seguridad de los datos de conformidad con lo previsto en el artículo 34 del Reglamento (UE) 2016/679 si el responsable del tratamiento hubiera sido requerido por la autoridad de protección de datos para llevar a cabo dicha notificación.

t) El tratamiento de datos personales sin haber llevado a cabo la evaluación del impacto de las operaciones de tratamiento en la protección de datos personales en los supuestos en que la misma sea exigible.

u) El tratamiento de datos personales sin haber consultado previamente a la autoridad de protección de datos en los casos en que dicha consulta resulta preceptiva conforme al artículo 36 del Reglamento (UE) 2016/679 o cuando la ley establezca la obligación de llevar a cabo esa consulta.

v) El incumplimiento de la obligación de designar un delegado de protección de datos cuando sea exigible su nombramiento de acuerdo con el artículo 37 del Reglamento (UE) 2016/679 y el artículo 34 de esta ley orgánica.

w) No posibilitar la efectiva participación del delegado de protección de datos en todas las cuestiones relativas a la protección de datos personales, no respaldarlo o interferir en el desempeño de sus funciones.

x) La utilización de un sello o certificación en materia de protección de datos que no haya sido otorgado por una entidad de certificación debidamente acreditada o en caso de que la vigencia del mismo hubiera expirado.

y) Obtener la acreditación como organismo de certificación presentando información inexacta sobre el cumplimiento de los requisitos exigidos por el artículo 43 del Reglamento (UE) 2016/679.

z) El desempeño de funciones que el Reglamento (UE) 2016/679 reserva a los organismos de certificación, sin haber sido debidamente acreditado conforme a lo establecido en el artículo 39 de esta ley orgánica.

aa) El incumplimiento por parte de un organismo de certificación de los principios y deberes a los que está sometido según lo previsto en los artículos 42 y 43 de Reglamento (UE) 2016/679.

ab) El desempeño de funciones que el artículo 41 del Reglamento (UE) 2016/679 reserva a los organismos de supervisión de códigos de conducta sin haber sido previamente acreditado por la autoridad de protección de datos competente.

ac) La falta de adopción por parte de los organismos acreditados de supervisión de un código de conducta de las medidas que resulten oportunas en caso que se hubiera producido una infracción del código, conforme exige el artículo 41.4 del Reglamento (UE) 2016/679.

Artículo 74. *Infracciones consideradas leves.*

Se consideran leves y prescribirán al año las restantes infracciones de carácter meramente formal de los artículos mencionados en los apartados 4 y 5 del artículo 83 del Reglamento (UE) 2016/679 y, en particular, las siguientes:

a) El incumplimiento del principio de transparencia de la información o el derecho de información del afectado por no facilitar toda la información exigida por los artículos 13 y 14 del Reglamento (UE) 2016/679.

b) La exigencia del pago de un canon para facilitar al afectado la información exigida por los artículos 13 y 14 del Reglamento (UE) 2016/679 o por atender las solicitudes de ejercicio de derechos de los afectados previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679, cuando así lo permita su artículo 12.5, si su cuantía excediese el importe de los costes afrontados para facilitar la información o realizar la actuación solicitada.

c) No atender las solicitudes de ejercicio de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, salvo que resultase de aplicación lo dispuesto en el artículo 72.1.k) de esta ley orgánica.

d) No atender los derechos de acceso, rectificación, supresión, limitación del tratamiento o a la portabilidad de los datos en tratamientos en los que no se requiere la identificación del afectado, cuando este, para el ejercicio de esos derechos, haya facilitado información adicional que permita su identificación, salvo que resultase de aplicación lo dispuesto en el artículo 73 c) de esta ley orgánica.

e) El incumplimiento de la obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento exigida por el artículo 19 del Reglamento (UE) 2016/679.

f) El incumplimiento de la obligación de informar al afectado, cuando así lo haya solicitado, de los destinatarios a los que se hayan comunicado los datos personales rectificados, suprimidos o respecto de los que se ha limitado el tratamiento.

g) El incumplimiento de la obligación de suprimir los datos referidos a una persona fallecida cuando ello fuera exigible conforme al artículo 3 de esta ley orgánica.

h) La falta de formalización por los corresponsables del tratamiento del acuerdo que determine las obligaciones, funciones y responsabilidades respectivas con respecto al

tratamiento de datos personales y sus relaciones con los afectados al que se refiere el artículo 26 del Reglamento (UE) 2016/679 o la inexactitud en la determinación de las mismas.

i) No poner a disposición de los afectados los aspectos esenciales del acuerdo formalizado entre los corresponsables del tratamiento, conforme exige el artículo 26.2 del Reglamento (UE) 2016/679.

j) La falta del cumplimiento de la obligación del encargado del tratamiento de informar al responsable del tratamiento acerca de la posible infracción por una instrucción recibida de este de las disposiciones del Reglamento (UE) 2016/679 o de esta ley orgánica, conforme a lo exigido por el artículo 28.3 del citado reglamento.

k) El incumplimiento por el encargado de las estipulaciones impuestas en el contrato o acto jurídico que regula el tratamiento o las instrucciones del responsable del tratamiento, salvo que esté legalmente obligado a ello conforme al Reglamento (UE) 2016/679 y a la presente ley orgánica o en los supuestos en que fuese necesario para evitar la infracción de la legislación en materia de protección de datos y se hubiese advertido de ello al responsable o al encargado del tratamiento.

l) Disponer de un Registro de actividades de tratamiento que no incorpore toda la información exigida por el artículo 30 del Reglamento (UE) 2016/679.

m) La notificación incompleta, tardía o defectuosa a la autoridad de protección de datos de la información relacionada con una violación de seguridad de los datos personales de conformidad con lo previsto en el artículo 33 del Reglamento (UE) 2016/679.

n) El incumplimiento de la obligación de documentar cualquier violación de seguridad, exigida por el artículo 33.5 del Reglamento (UE) 2016/679.

ñ) El incumplimiento del deber de comunicación al afectado de una violación de la seguridad de los datos que entrañe un alto riesgo para los derechos y libertades de los afectados, conforme a lo exigido por el artículo 34 del Reglamento (UE) 2016/679, salvo que resulte de aplicación lo previsto en el artículo 73 s) de esta ley orgánica.

o) Facilitar información inexacta a la Autoridad de protección de datos, en los supuestos en los que el responsable del tratamiento deba elevarle una consulta previa, conforme al artículo 36 del Reglamento (UE) 2016/679.

p) No publicar los datos de contacto del delegado de protección de datos, o no comunicarlos a la autoridad de protección de datos, cuando su nombramiento sea exigible de acuerdo con el artículo 37 del Reglamento (UE) 2016/679 y el artículo 34 de esta ley orgánica.

q) El incumplimiento por los organismos de certificación de la obligación de informar a la autoridad de protección de datos de la expedición, renovación o retirada de una certificación, conforme a lo exigido por los apartados 1 y 5 del artículo 43 del Reglamento (UE) 2016/679.

r) El incumplimiento por parte de los organismos acreditados de supervisión de un código de conducta de la obligación de informar a las autoridades de protección de datos acerca de las medidas que resulten oportunas en caso de infracción del código, conforme exige el artículo 41.4 del Reglamento (UE) 2016/679.

Artículo 75. *Interrupción de la prescripción de la infracción.*

Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador, reiniciándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de seis meses por causas no imputables al presunto infractor.

Cuando la Agencia Española de Protección de Datos ostente la condición de autoridad de control principal y deba seguirse el procedimiento previsto en el artículo 60 del Reglamento (UE) 2016/679 interrumpirá la prescripción el conocimiento formal por el interesado del acuerdo de inicio.

Artículo 76. *Sanciones y medidas correctivas.*

1. Las sanciones previstas en los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679 se aplicarán teniendo en cuenta los criterios de graduación establecidos en el apartado 2 del citado artículo.

2. De acuerdo a lo previsto en el artículo 83.2.k) del Reglamento (UE) 2016/679 también podrán tenerse en cuenta:

a) El carácter continuado de la infracción.
b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.
c) Los beneficios obtenidos como consecuencia de la comisión de la infracción.
d) La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.
e) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.
f) La afectación a los derechos de los menores.
g) Disponer, cuando no fuere obligatorio, de un delegado de protección de datos.
h) El sometimiento por parte del responsable o encargado, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias entre aquellos y cualquier interesado.

3. Será posible, complementaria o alternativamente, la adopción, cuando proceda, de las restantes medidas correctivas a las que se refiere el artículo 83.2 del Reglamento (UE) 2016/679.
4. Será objeto de publicación en el Boletín Oficial del Estado la información que identifique al infractor, la infracción cometida y el importe de la sanción impuesta cuando la autoridad competente sea la Agencia Española de Protección de Datos, la sanción fuese superior a un millón de euros y el infractor sea una persona jurídica.
Cuando la autoridad competente para imponer la sanción sea una autoridad autonómica de protección de datos, se estará a su normativa de aplicación.

Artículo 77. *Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento.*

1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:

a) Los órganos constitucionales o con relevancia constitucional y las instituciones de las comunidades autónomas análogas a los mismos.
b) Los órganos jurisdiccionales.
c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.
d) Los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas.
e) Las autoridades administrativas independientes.
f) El Banco de España.
g) Las corporaciones de Derecho público cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de derecho público.
h) Las fundaciones del sector público.
i) Las Universidades Públicas.
j) Los consorcios.
k) Los grupos parlamentarios de las Cortes Generales y las Asambleas Legislativas autonómicas, así como los grupos políticos de las Corporaciones Locales.

2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución declarando la infracción y estableciendo, en su caso, las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido, con excepción de la prevista en el artículo 58.2.i del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.
La resolución se notificará al responsable o encargado del tratamiento, al órgano del que dependa jerárquicamente, en su caso, y a los afectados que tuvieran la condición de interesado, en su caso.

3. Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.

Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda.

4. Se deberán comunicar a la autoridad de protección de datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

5. Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo.

6. Cuando la autoridad competente sea la Agencia Española de Protección de Datos, esta publicará en su página web con la debida separación las resoluciones referidas a las entidades del apartado 1 de este artículo, con expresa indicación de la identidad del responsable o encargado del tratamiento que hubiera cometido la infracción.

Cuando la competencia corresponda a una autoridad autonómica de protección de datos se estará, en cuanto a la publicidad de estas resoluciones, a lo que disponga su normativa específica.

Artículo 78. *Prescripción de las sanciones.*

1. Las sanciones impuestas en aplicación del Reglamento (UE) 2016/679 y de esta ley orgánica prescriben en los siguientes plazos:

a) Las sanciones por importe igual o inferior a 40.000 euros, prescriben en el plazo de un año.

b) Las sanciones por importe comprendido entre 40.001 y 300.000 euros prescriben a los dos años.

c) Las sanciones por un importe superior a 300.000 euros prescriben a los tres años.

2. El plazo de prescripción de las sanciones comenzará a contarse desde el día siguiente a aquel en que sea ejecutable la resolución por la que se impone la sanción o haya transcurrido el plazo para recurrirla.

3. La prescripción se interrumpirá por la iniciación, con conocimiento del interesado, del procedimiento de ejecución, volviendo a transcurrir el plazo si el mismo está paralizado durante más de seis meses por causa no imputable al infractor.

TÍTULO X

Garantía de los derechos digitales

Artículo 79. *Los derechos en la Era digital.*

Los derechos y libertades consagrados en la Constitución y en los Tratados y Convenios Internacionales en que España sea parte son plenamente aplicables en Internet. Los prestadores de servicios de la sociedad de la información y los proveedores de servicios de Internet contribuirán a garantizar su aplicación.

Artículo 80. *Derecho a la neutralidad de Internet.*

Los usuarios tienen derecho a la neutralidad de Internet. Los proveedores de servicios de Internet proporcionarán una oferta transparente de servicios sin discriminación por motivos técnicos o económicos.

Artículo 81. *Derecho de acceso universal a Internet.*

1. Todos tienen derecho a acceder a Internet independientemente de su condición personal, social, económica o geográfica.
2. Se garantizará un acceso universal, asequible, de calidad y no discriminatorio para toda la población.
3. El acceso a Internet de hombres y mujeres procurará la superación de la brecha de género tanto en el ámbito personal como laboral.
4. El acceso a Internet procurará la superación de la brecha generacional mediante acciones dirigidas a la formación y el acceso a las personas mayores.
5. La garantía efectiva del derecho de acceso a Internet atenderá la realidad específica de los entornos rurales.
6. El acceso a Internet deberá garantizar condiciones de igualdad para las personas que cuenten con necesidades especiales.

Artículo 82. *Derecho a la seguridad digital.*

Los usuarios tienen derecho a la seguridad de las comunicaciones que transmitan y reciban a través de Internet. Los proveedores de servicios de Internet informarán a los usuarios de sus derechos.

Artículo 83. *Derecho a la educación digital.*

1. El sistema educativo garantizará la plena inserción del alumnado en la sociedad digital y el aprendizaje de un consumo responsable y un uso crítico y seguro de los medios digitales y respetuoso con la dignidad humana, la justicia social y la sostenibilidad medioambiental, los valores constitucionales, los derechos fundamentales y, particularmente con el respeto y la garantía de la intimidad personal y familiar y la protección de datos personales. Las actuaciones realizadas en este ámbito tendrán carácter inclusivo, en particular en lo que respecta al alumnado con necesidades educativas especiales.

Las Administraciones educativas deberán incluir en el desarrollo del currículo la competencia digital a la que se refiere el apartado anterior, así como los elementos relacionados con las situaciones de riesgo derivadas de la inadecuada utilización de las TIC, con especial atención a las situaciones de violencia en la red.

2. El profesorado recibirá las competencias digitales y la formación necesaria para la enseñanza y transmisión de los valores y derechos referidos en el apartado anterior.
3. Los planes de estudio de los títulos universitarios, en especial, aquellos que habiliten para el desempeño profesional en la formación del alumnado, garantizarán la formación en el uso y seguridad de los medios digitales y en la garantía de los derechos fundamentales en Internet.
4. Las Administraciones Públicas incorporarán a los temarios de las pruebas de acceso a los cuerpos superiores y a aquéllos en que habitualmente se desempeñen funciones que impliquen el acceso a datos personales materias relacionadas con la garantía de los derechos digitales y en particular el de protección de datos.

Artículo 84. *Protección de los menores en Internet.*

1. Los padres, madres, tutores, curadores o representantes legales procurarán que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales y de los servicios de la sociedad de la información a fin de garantizar el adecuado desarrollo de su personalidad y preservar su dignidad y sus derechos fundamentales.
2. La utilización o difusión de imágenes o información personal de menores en las redes sociales y servicios de la sociedad de la información equivalentes que puedan implicar una intromisión ilegítima en sus derechos fundamentales determinará la intervención del Ministerio Fiscal, que instará las medidas cautelares y de protección previstas en la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor.

Artículo 85. *Derecho de rectificación en Internet.*

1. Todos tienen derecho a la libertad de expresión en Internet.

2. Los responsables de redes sociales y servicios equivalentes adoptarán protocolos adecuados para posibilitar el ejercicio del derecho de rectificación ante los usuarios que difundan contenidos que atenten contra el derecho al honor, la intimidad personal y familiar en Internet y el derecho a comunicar o recibir libremente información veraz, atendiendo a los requisitos y procedimientos previstos en la Ley Orgánica 2/1984, de 26 de marzo, reguladora del derecho de rectificación.

Cuando los medios de comunicación digitales deban atender la solicitud de rectificación formulada contra ellos deberán proceder a la publicación en sus archivos digitales de un aviso aclaratorio que ponga de manifiesto que la noticia original no refleja la situación actual del individuo. Dicho aviso deberá aparecer en lugar visible junto con la información original.

Artículo 86. *Derecho a la actualización de informaciones en medios de comunicación digitales.*

Toda persona tiene derecho a solicitar motivadamente de los medios de comunicación digitales la inclusión de un aviso de actualización suficientemente visible junto a las noticias que le conciernan cuando la información contenida en la noticia original no refleje su situación actual como consecuencia de circunstancias que hubieran tenido lugar después de la publicación, causándole un perjuicio.

En particular, procederá la inclusión de dicho aviso cuando las informaciones originales se refieran a actuaciones policiales o judiciales que se hayan visto afectadas en beneficio del interesado como consecuencia de decisiones judiciales posteriores. En este caso, el aviso hará referencia a la decisión posterior.

Artículo 87. *Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral.*

1. Los trabajadores y los empleados públicos tendrán derecho a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por su empleador.

2. El empleador podrá acceder a los contenidos derivados del uso de medios digitales facilitados a los trabajadores a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos.

3. Los empleadores deberán establecer criterios de utilización de los dispositivos digitales respetando en todo caso los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente. En su elaboración deberán participar los representantes de los trabajadores.

El acceso por el empleador al contenido de dispositivos digitales respecto de los que haya admitido su uso con fines privados requerirá que se especifiquen de modo preciso los usos autorizados y se establezcan garantías para preservar la intimidad de los trabajadores, tales como, en su caso, la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados.

Los trabajadores deberán ser informados de los criterios de utilización a los que se refiere este apartado.

Artículo 88. *Derecho a la desconexión digital en el ámbito laboral.*

1. Los trabajadores y los empleados públicos tendrán derecho a la desconexión digital a fin de garantizar, fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar.

2. Las modalidades de ejercicio de este derecho atenderán a la naturaleza y objeto de la relación laboral, potenciarán el derecho a la conciliación de la actividad laboral y la vida personal y familiar y se sujetarán a lo establecido en la negociación colectiva o, en su defecto, a lo acordado entre la empresa y los representantes de los trabajadores.

3. El empleador, previa audiencia de los representantes de los trabajadores, elaborará una política interna dirigida a trabajadores, incluidos los que ocupen puestos directivos, en la que definirán las modalidades de ejercicio del derecho a la desconexión y las acciones de formación y de sensibilización del personal sobre un uso razonable de las herramientas tecnológicas que evite el riesgo de fatiga informática. En particular, se preservará el derecho a la desconexión digital en los supuestos de realización total o parcial del trabajo a distancia

así como en el domicilio del empleado vinculado al uso con fines laborales de herramientas tecnológicas.

Artículo 89. *Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo.*

1. Los empleadores podrán tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo. Los empleadores habrán de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de esta medida.

En el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores o los empleados públicos se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el artículo 22.4 de esta ley orgánica.

2. En ningún caso se admitirá la instalación de sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y análogos.

3. La utilización de sistemas similares a los referidos en los apartados anteriores para la grabación de sonidos en el lugar de trabajo se admitirá únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando el principio de proporcionalidad, el de intervención mínima y las garantías previstas en los apartados anteriores. La supresión de los sonidos conservados por estos sistemas de grabación se realizará atendiendo a lo dispuesto en el apartado 3 del artículo 22 de esta ley.

Artículo 90. *Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral.*

1. Los empleadores podrán tratar los datos obtenidos a través de sistemas de geolocalización para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo.

2. Con carácter previo, los empleadores habrán de informar de forma expresa, clara e inequívoca a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de la existencia y características de estos dispositivos. Igualmente deberán informarles acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión.

Artículo 91. *Derechos digitales en la negociación colectiva.*

Los convenios colectivos podrán establecer garantías adicionales de los derechos y libertades relacionados con el tratamiento de los datos personales de los trabajadores y la salvaguarda de derechos digitales en el ámbito laboral.

Artículo 92. *Protección de datos de los menores en Internet.*

Los centros educativos y cualesquiera personas físicas o jurídicas que desarrollen actividades en las que participen menores de edad garantizarán la protección del interés superior del menor y sus derechos fundamentales, especialmente el derecho a la protección de datos personales, en la publicación o difusión de sus datos personales a través de servicios de la sociedad de la información.

Cuando dicha publicación o difusión fuera a tener lugar a través de servicios de redes sociales o servicios equivalentes deberán contar con el consentimiento del menor o sus representantes legales, conforme a lo prescrito en el artículo 7 de esta ley orgánica.

Artículo 93. *Derecho al olvido en búsquedas de Internet.*

1. Toda persona tiene derecho a que los motores de búsqueda en Internet eliminen de las listas de resultados que se obtuvieran tras una búsqueda efectuada a partir de su nombre los enlaces publicados que contuvieran información relativa a esa persona cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información.

Del mismo modo deberá procederse cuando las circunstancias personales que en su caso invocase el afectado evidenciasen la prevalencia de sus derechos sobre el mantenimiento de los enlaces por el servicio de búsqueda en Internet.

Este derecho subsistirá aun cuando fuera lícita la conservación de la información publicada en el sitio web al que se dirigiera el enlace y no se procediese por la misma a su borrado previo o simultáneo.

2. El ejercicio del derecho al que se refiere este artículo no impedirá el acceso a la información publicada en el sitio web a través de la utilización de otros criterios de búsqueda distintos del nombre de quien ejerciera el derecho.

Artículo 94. *Derecho al olvido en servicios de redes sociales y servicios equivalentes.*

1. Toda persona tiene derecho a que sean suprimidos, a su simple solicitud, los datos personales que hubiese facilitado para su publicación por servicios de redes sociales y servicios de la sociedad de la información equivalentes.

2. Toda persona tiene derecho a que sean suprimidos los datos personales que le conciernan y que hubiesen sido facilitados por terceros para su publicación por los servicios de redes sociales y servicios de la sociedad de la información equivalentes cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información.

Del mismo modo deberá procederse a la supresión de dichos datos cuando las circunstancias personales que en su caso invocase el afectado evidenciasen la prevalencia de sus derechos sobre el mantenimiento de los datos por el servicio.

Se exceptúan de lo dispuesto en este apartado los datos que hubiesen sido facilitados por personas físicas en el ejercicio de actividades personales o domésticas.

3. En caso de que el derecho se ejercitase por un afectado respecto de datos que hubiesen sido facilitados al servicio, por él o por terceros, durante su minoría de edad, el prestador deberá proceder sin dilación a su supresión por su simple solicitud, sin necesidad de que concurran las circunstancias mencionadas en el apartado 2.

Artículo 95. *Derecho de portabilidad en servicios de redes sociales y servicios equivalentes.*

Los usuarios de servicios de redes sociales y servicios de la sociedad de la información equivalentes tendrán derecho a recibir y transmitir los contenidos que hubieran facilitado a los prestadores de dichos servicios, así como a que los prestadores los transmitan directamente a otro prestador designado por el usuario, siempre que sea técnicamente posible.

Los prestadores podrán conservar, sin difundirla a través de Internet, copia de los contenidos cuando dicha conservación sea necesaria para el cumplimiento de una obligación legal.

Artículo 96. *Derecho al testamento digital.*

1. El acceso a contenidos gestionados por prestadores de servicios de la sociedad de la información sobre personas fallecidas se regirá por las siguientes reglas:

a) Las personas vinculadas al fallecido por razones familiares o de hecho, así como sus herederos podrán dirigirse a los prestadores de servicios de la sociedad de la información al

objeto de acceder a dichos contenidos e impartirles las instrucciones que estimen oportunas sobre su utilización, destino o supresión.

Como excepción, las personas mencionadas no podrán acceder a los contenidos del causante, ni solicitar su modificación o eliminación, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley. Dicha prohibición no afectará al derecho de los herederos a acceder a los contenidos que pudiesen formar parte del caudal relicto.

b) El albacea testamentario así como aquella persona o institución a la que el fallecido hubiese designado expresamente para ello también podrá solicitar, con arreglo a las instrucciones recibidas, el acceso a los contenidos con vistas a dar cumplimiento a tales instrucciones.

c) En caso de personas fallecidas menores de edad, estas facultades podrán ejercerse también por sus representantes legales o, en el marco de sus competencias, por el Ministerio Fiscal, que podrá actuar de oficio o a instancia de cualquier persona física o jurídica interesada.

d) En caso de fallecimiento de personas con discapacidad, estas facultades podrán ejercerse también, además de por quienes señala la letra anterior, por quienes hubiesen sido designados para el ejercicio de funciones de apoyo si tales facultades se entendieran comprendidas en las medidas de apoyo prestadas por el designado.

2. Las personas legitimadas en el apartado anterior podrán decidir acerca del mantenimiento o eliminación de los perfiles personales de personas fallecidas en redes sociales o servicios equivalentes, a menos que el fallecido hubiera decidido acerca de esta circunstancia, en cuyo caso se estará a sus instrucciones.

El responsable del servicio al que se le comunique, con arreglo al párrafo anterior, la solicitud de eliminación del perfil, deberá proceder sin dilación a la misma.

3. Mediante real decreto se establecerán los requisitos y condiciones para acreditar la validez y vigencia de los mandatos e instrucciones y, en su caso, el registro de los mismos, que podrá coincidir con el previsto en el artículo 3 de esta ley orgánica.

4. Lo establecido en este artículo en relación con las personas fallecidas en las comunidades autónomas con derecho civil, foral o especial, propio se regirá por lo establecido por estas dentro de su ámbito de aplicación.

Artículo 97. *Políticas de impulso de los derechos digitales.*

1. El Gobierno, en colaboración con las comunidades autónomas, elaborará un Plan de Acceso a Internet con los siguientes objetivos:

a) superar las brechas digitales y garantizar el acceso a Internet de colectivos vulnerables o con necesidades especiales y de entornos familiares y sociales económicamente desfavorecidos mediante, entre otras medidas, un bono social de acceso a Internet;

b) impulsar la existencia de espacios de conexión de acceso público; y

c) fomentar medidas educativas que promuevan la formación en competencias y habilidades digitales básicas a personas y colectivos en riesgo de exclusión digital y la capacidad de todas las personas para realizar un uso autónomo y responsable de Internet y de las tecnologías digitales.

2. Asimismo se aprobará un Plan de Actuación dirigido a promover las acciones de formación, difusión y concienciación necesarias para lograr que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales y de las redes sociales y de los servicios de la sociedad de la información equivalentes de Internet con la finalidad de garantizar su adecuado desarrollo de la personalidad y de preservar su dignidad y derechos fundamentales.

3. El Gobierno presentará un informe anual ante la comisión parlamentaria correspondiente del Congreso de los Diputados en el que se dará cuenta de la evolución de los derechos, garantías y mandatos contemplados en el presente Título y de las medidas necesarias para promover su impulso y efectividad.

Disposición adicional primera. *Medidas de seguridad en el ámbito del sector público.*

1. El Esquema Nacional de Seguridad incluirá las medidas que deban implantarse en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679.

2. Los responsables enumerados en el artículo 77.1 de esta ley orgánica deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado.

En los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad.

Disposición adicional segunda. *Protección de datos y transparencia y acceso a la información pública.*

La publicidad activa y el acceso a la información pública regulados por el Título I de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, así como las obligaciones de publicidad activa establecidas por la legislación autonómica, se someterán, cuando la información contenga datos personales, a lo dispuesto en los artículos 5.3 y 15 de la Ley 19/2013, en el Reglamento (UE) 2016/679 y en la presente ley orgánica.

Disposición adicional tercera. *Cómputo de plazos.*

Los plazos establecidos en el Reglamento (UE) 2016/679 o en esta ley orgánica, con independencia de que se refieran a relaciones entre particulares o con entidades del sector público, se regirán por las siguientes reglas:

a) Cuando los plazos se señalen por días, se entiende que estos son hábiles, excluyéndose del cómputo los sábados, los domingos y los declarados festivos.

b) Si el plazo se fija en semanas, concluirá el mismo día de la semana en que se produjo el hecho que determina su iniciación en la semana de vencimiento.

c) Si el plazo se fija en meses o años, concluirá el mismo día en que se produjo el hecho que determina su iniciación en el mes o el año de vencimiento. Si en el mes de vencimiento no hubiera día equivalente a aquel en que comienza el cómputo, se entenderá que el plazo expira el último día del mes.

d) Cuando el último día del plazo sea inhábil, se entenderá prorrogado al primer día hábil siguiente.

Disposición adicional cuarta. *Procedimiento en relación con las competencias atribuidas a la Agencia Española de Protección de Datos por otras leyes.*

Lo dispuesto en el Título VIII y en sus normas de desarrollo será de aplicación a los procedimientos que la Agencia Española de Protección de Datos hubiera de tramitar en ejercicio de las competencias que le fueran atribuidas por otras leyes.

Disposición adicional quinta. *Autorización judicial en relación con decisiones de la Comisión Europea en materia de transferencia internacional de datos.*

1. Cuando una autoridad de protección de datos considerase que una decisión de la Comisión Europea en materia de transferencia internacional de datos, de cuya validez dependiese la resolución de un procedimiento concreto, infringiese lo dispuesto en el Reglamento (UE) 2016/679, menoscabando el derecho fundamental a la protección de datos, acordará inmediatamente la suspensión del procedimiento, a fin de solicitar del órgano judicial autorización para declararlo así en el seno del procedimiento del que esté conociendo. Dicha suspensión deberá ser confirmada, modificada o levantada en el acuerdo de admisión o inadmisión a trámite de la solicitud de la autoridad de protección de datos dirigida al tribunal competente.

Las decisiones de la Comisión Europea a las que puede resultar de aplicación este cauce son:

a) aquellas que declaren el nivel adecuado de protección de un tercer país u organización internacional, en virtud del artículo 45 del Reglamento (UE) 2016/679;

b) aquellas por las que se aprueben cláusulas tipo de protección de datos para la realización de transferencias internacionales de datos, o

c) aquellas que declaren la validez de los códigos de conducta a tal efecto.

2. La autorización a la que se refiere esta disposición solamente podrá ser concedida si, previo planteamiento de cuestión prejudicial de validez en los términos del artículo 267 del Tratado de Funcionamiento de la Unión Europea, la decisión de la Comisión Europea cuestionada fuera declarada inválida por el Tribunal de Justicia de la Unión Europea.

Disposición adicional sexta. *Incorporación de deudas a sistemas de información crediticia.*

No se incorporarán a los sistemas de información crediticia a los que se refiere el artículo 20.1 de esta ley orgánica deudas en que la cuantía del principal sea inferior a cincuenta euros.

El Gobierno, mediante real decreto, podrá actualizar esta cuantía.

Disposición adicional séptima. *Identificación de los interesados en las notificaciones por medio de anuncios y publicaciones de actos administrativos.*

1. Cuando sea necesaria la publicación de un acto administrativo que contuviese datos personales del afectado, se identificará al mismo mediante su nombre y apellidos, añadiendo cuatro cifras numéricas aleatorias del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente. Cuando la publicación se refiera a una pluralidad de afectados estas cifras aleatorias deberán alternarse.

Cuando se trate de la notificación por medio de anuncios, particularmente en los supuestos a los que se refiere el artículo 44 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, se identificará al afectado exclusivamente mediante el número completo de su documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente.

Cuando el afectado careciera de cualquiera de los documentos mencionados en los dos párrafos anteriores, se identificará al afectado únicamente mediante su nombre y apellidos. En ningún caso debe publicarse el nombre y apellidos de manera conjunta con el número completo del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente.

2. A fin de prevenir riesgos para víctimas de violencia de género, el Gobierno impulsará la elaboración de un protocolo de colaboración que defina procedimientos seguros de publicación y notificación de actos administrativos, con la participación de los órganos con competencia en la materia.

Disposición adicional octava. *Potestad de verificación de las Administraciones Públicas.*

Cuando se formulen solicitudes por cualquier medio en las que el interesado declare datos personales que obren en poder de las Administraciones Públicas, el órgano destinatario de la solicitud podrá efectuar en el ejercicio de sus competencias las verificaciones necesarias para comprobar la exactitud de los datos.

Disposición adicional novena. *Tratamiento de datos personales en relación con la notificación de incidentes de seguridad.*

Cuando, de conformidad con lo dispuesto en la legislación nacional que resulte de aplicación, deban notificarse incidentes de seguridad, las autoridades públicas competentes, equipos de respuesta a emergencias informáticas (CERT), equipos de respuesta a incidentes de seguridad informática (CSIRT), proveedores de redes y servicios de comunicaciones electrónicas y proveedores de tecnologías y servicios de seguridad, podrán tratar los datos personales contenidos en tales notificaciones, exclusivamente durante el tiempo y alcance necesarios para su análisis, detección, protección y respuesta ante

incidentes y adoptando las medidas de seguridad adecuadas y proporcionadas al nivel de riesgo determinado.

Disposición adicional décima. *Comunicaciones de datos por los sujetos enumerados en el artículo 77.1.*

Los responsables enumerados en el artículo 77.1 de esta ley orgánica podrán comunicar los datos personales que les sean solicitados por sujetos de derecho privado cuando cuenten con el consentimiento de los afectados o aprecien que concurre en los solicitantes un interés legítimo que prevalezca sobre los derechos e intereses de los afectados conforme a lo establecido en el artículo 6.1 f) del Reglamento (UE) 2016/679.

Disposición adicional undécima. *Privacidad en las comunicaciones electrónicas.*

Lo dispuesto en la presente ley orgánica se entenderá sin perjuicio de la aplicación de las normas de Derecho interno y de la Unión Europea reguladoras de la privacidad en el sector de las comunicaciones electrónicas, sin imponer obligaciones adicionales a las personas físicas o jurídicas en materia de tratamiento en el marco de la prestación de servicios públicos de comunicaciones electrónicas en redes públicas de comunicación en ámbitos en los que estén sujetas a obligaciones específicas establecidas en dichas normas.

Disposición adicional duodécima. *Disposiciones específicas aplicables a los tratamientos de los registros de personal del sector público.*

1. Los tratamientos de los registros de personal del sector público se entenderán realizados en el ejercicio de poderes públicos conferidos a sus responsables, de acuerdo con lo previsto en el artículo 6.1.e) del Reglamento (UE) 2016/679.
2. Los registros de personal del sector público podrán tratar datos personales relativos a infracciones y condenas penales e infracciones y sanciones administrativas, limitándose a los datos estrictamente necesarios para el cumplimiento de sus fines.
3. De acuerdo con lo previsto en el artículo 18.2 del Reglamento (UE) 2016/679, y por considerarlo una razón de interés público importante, los datos cuyo tratamiento se haya limitado en virtud del artículo 18.1 del citado reglamento, podrán ser objeto de tratamiento cuando sea necesario para el desarrollo de los procedimientos de personal.

Disposición adicional decimotercera. *Transferencias internacionales de datos tributarios.*

Las transferencias de datos tributarios entre el Reino de España y otros Estados o entidades internacionales o supranacionales, se regularán por los términos y con los límites establecidos en la normativa sobre asistencia mutua entre los Estados de la Unión Europea, o en el marco de los convenios para evitar la doble imposición o de otros convenios internacionales, así como por las normas sobre la asistencia mutua establecidas en el Capítulo VI del Título III de la Ley 58/2003, de 17 de diciembre, General Tributaria.

Disposición adicional decimocuarta. *Normas dictadas en desarrollo del artículo 13 de la Directiva 95/46/CE.*

Las normas dictadas en aplicación del artículo 13 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, que hubiesen entrado en vigor con anterioridad a 25 de mayo de 2018, y en particular los artículos 23 y 24 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, siguen vigentes en tanto no sean expresamente modificadas, sustituidas o derogadas.

Disposición adicional decimoquinta. *Requerimiento de información por parte de la Comisión Nacional del Mercado de Valores.*

Cuando no haya podido obtener por otros medios la información necesaria para realizar sus labores de supervisión e inspección relacionadas con la detección de delitos graves, la Comisión Nacional del Mercado de Valores podrá recabar de los operadores que presten

servicios de comunicaciones electrónicas disponibles al público y de los prestadores de servicios de la sociedad de la información, los datos que obren en su poder relativos a la comunicación electrónica o servicio de la sociedad de la información proporcionados por dichos prestadores que sean distintos a su contenido y resulten imprescindibles para el ejercicio de dichas labores.

La cesión de estos datos requerirá la previa obtención de autorización judicial otorgada conforme a las normas procesales.

Disposición adicional decimosexta. *Prácticas agresivas en materia de protección de datos.*

A los efectos previstos en el artículo 8 de la Ley 3/1991, de 10 de enero, de Competencia Desleal, se consideran prácticas agresivas las siguientes:

a) Actuar con intención de suplantar la identidad de la Agencia Española de Protección de Datos o de una autoridad autonómica de protección de datos en la realización de cualquier comunicación a los responsables y encargados de los tratamientos o a los interesados.

b) Generar la apariencia de que se está actuando en nombre, por cuenta o en colaboración con la Agencia Española de Protección de Datos o una autoridad autonómica de protección de datos en la realización de cualquier comunicación a los responsables y encargados de los tratamientos en que la remitente ofrezca sus productos o servicios.

c) Realizar prácticas comerciales en las que se coarte el poder de decisión de los destinatarios mediante la referencia a la posible imposición de sanciones por incumplimiento de la normativa de protección de datos personales.

d) Ofrecer cualquier tipo de documento por el que se pretenda crear una apariencia de cumplimiento de las disposiciones de protección de datos de forma complementaria a la realización de acciones formativas sin haber llevado a cabo las actuaciones necesarias para verificar que dicho cumplimiento se produce efectivamente.

e) Asumir, sin designación expresa del responsable o el encargado del tratamiento, la función de delegado de protección de datos y comunicarse en tal condición con la Agencia Española de Protección de Datos o las autoridades autonómicas de protección de datos.

Disposición adicional decimoséptima. *Tratamientos de datos de salud.*

1. Se encuentran amparados en las letras g), h), i) y j) del artículo 9.2 del Reglamento (UE) 2016/679 los tratamientos de datos relacionados con la salud y de datos genéticos que estén regulados en las siguientes leyes y sus disposiciones de desarrollo:

a) La Ley 14/1986, de 25 de abril, General de Sanidad.

b) La Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales.

c) La Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

d) La Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.

e) La Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias.

f) La Ley 14/2007, de 3 de julio, de Investigación biomédica.

g) La Ley 33/2011, de 4 de octubre, General de Salud Pública.

h) La Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.

i) El texto refundido de la Ley de garantías y uso racional de los 105 medicamentos y productos sanitarios, aprobado por Real Decreto Legislativo 1/2015, de 24 de julio.

j) El texto refundido de la Ley General de derechos de las personas con discapacidad y de su inclusión social, aprobado por Real Decreto Legislativo 1/2013 de 29 de noviembre.

2. El tratamiento de datos en la investigación en salud se regirá por los siguientes criterios:

a) El interesado o, en su caso, su representante legal podrá otorgar el consentimiento para el uso de sus datos con fines de investigación en salud y, en particular, la biomédica. Tales finalidades podrán abarcar categorías relacionadas con áreas generales vinculadas a una especialidad médica o investigadora.

b) Las autoridades sanitarias e instituciones públicas con competencias en vigilancia de la salud pública podrán llevar a cabo estudios científicos sin el consentimiento de los afectados en situaciones de excepcional relevancia y gravedad para la salud pública.

c) Se considerará lícita y compatible la reutilización de datos personales con fines de investigación en materia de salud y biomédica cuando, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen los datos para finalidades o áreas de investigación relacionadas con el área en la que se integrase científicamente el estudio inicial.

En tales casos, los responsables deberán publicar la información establecida por el artículo 13 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, en un lugar fácilmente accesible de la página web corporativa del centro donde se realice la investigación o estudio clínico, y, en su caso, en la del promotor, y notificar la existencia de esta información por medios electrónicos a los afectados. Cuando estos carezcan de medios para acceder a tal información, podrán solicitar su remisión en otro formato.

Para los tratamientos previstos en esta letra, se requerirá informe previo favorable del comité de ética de la investigación.

d) Se considera lícito el uso de datos personales seudonimizados con fines de investigación en salud y, en particular, biomédica.

El uso de datos personales seudonimizados con fines de investigación en salud pública y biomédica requerirá:

1.º Una separación técnica y funcional entre el equipo investigador y quienes realicen la seudonimización y conserven la información que posibilite la reidentificación.

2.º Que los datos seudonimizados únicamente sean accesibles al equipo de investigación cuando:

i) Exista un compromiso expreso de confidencialidad y de no realizar ninguna actividad de reidentificación.

ii) Se adopten medidas de seguridad específicas para evitar la reidentificación y el acceso de terceros no autorizados.

Podrá procederse a la reidentificación de los datos en su origen, cuando con motivo de una investigación que utilice datos seudonimizados, se aprecie la existencia de un peligro real y concreto para la seguridad o salud de una persona o grupo de personas, o una amenaza grave para sus derechos o sea necesaria para garantizar una adecuada asistencia sanitaria.

e) Cuando se traten datos personales con fines de investigación en salud, y en particular la biomédica, a los efectos del artículo 89.2 del Reglamento (UE) 2016/679, podrán excepcionarse los derechos de los afectados previstos en los artículos 15, 16, 18 y 21 del Reglamento (EU) 2016/679 cuando:

1.º Los citados derechos se ejerzan directamente ante los investigadores o centros de investigación que utilicen datos anonimizados o seudonimizados.

2.º El ejercicio de tales derechos se refiera a los resultados de la investigación.

3.º La investigación tenga por objeto un interés público esencial relacionado con la seguridad del Estado, la defensa, la seguridad pública u otros objetivos importantes de interés público general, siempre que en este último caso la excepción esté expresamente recogida por una norma con rango de Ley.

f) Cuando conforme a lo previsto por el artículo 89 del Reglamento (UE) 2016/679, se lleve a cabo un tratamiento con fines de investigación en salud pública y, en particular, biomédica se procederá a:

1.º Realizar una evaluación de impacto que determine los riesgos derivados del tratamiento en los supuestos previstos en el artículo 35 del Reglamento (UE) 2016/679 o en los establecidos por la autoridad de control. Esta evaluación incluirá de modo específico los riesgos de reidentificación vinculados a la anonimización o seudonimización de los datos.

2.º Someter la investigación científica a las normas de calidad y, en su caso, a las directrices internacionales sobre buena práctica clínica.

3.º Adoptar, en su caso, medidas dirigidas a garantizar que los investigadores no acceden a datos de identificación de los interesados.

4.º Designar un representante legal establecido en la Unión Europea, conforme al artículo 74 del Reglamento (UE) 536/2014, si el promotor de un ensayo clínico no está establecido en la Unión Europea. Dicho representante legal podrá coincidir con el previsto en el artículo 27.1 del Reglamento (UE) 2016/679.

g) El uso de datos personales seudonimizados con fines de investigación en salud pública y, en particular, biomédica deberá ser sometido al informe previo del comité de ética de la investigación previsto en la normativa sectorial.

En defecto de la existencia del mencionado Comité, la entidad responsable de la investigación requerirá informe previo del delegado de protección de datos o, en su defecto, de un experto con los conocimientos previos en el artículo 37.5 del Reglamento (UE) 2016/679.

h) En el plazo máximo de un año desde la entrada en vigor de esta ley, los comités de ética de la investigación, en el ámbito de la salud, biomédico o del medicamento, deberán integrar entre sus miembros un delegado de protección de datos o, en su defecto, un experto con conocimientos suficientes del Reglamento (UE) 2016/679 cuando se ocupen de actividades de investigación que comporten el tratamiento de datos personales o de datos seudonimizados o anonimizados.

Disposición adicional decimoctava. *Criterios de seguridad.*

La Agencia Española de Protección de Datos desarrollará, con la colaboración, cuando sea precisa, de todos los actores implicados, las herramientas, guías, directrices y orientaciones que resulten precisas para dotar a los profesionales, microempresas y pequeñas y medianas empresas de pautas adecuadas para el cumplimiento de las obligaciones de responsabilidad activa establecidas en el Título IV del Reglamento (UE) 2016/679 y en el Título V de esta ley orgánica.

Disposición adicional decimonovena. *Derechos de los menores ante Internet.*

En el plazo de un año desde la entrada en vigor de esta ley orgánica, el Gobierno remitirá al Congreso de los Diputados un proyecto de ley dirigido específicamente a garantizar los derechos de los menores ante el impacto de Internet, con el fin de garantizar su seguridad y luchar contra la discriminación y la violencia que sobre los mismos es ejercida mediante las nuevas tecnologías.

Disposición adicional vigésima. *Especialidades del régimen jurídico de la Agencia Española de Protección de Datos.*

1. No será de aplicación a la Agencia Española de Protección de Datos el artículo 50.2.c) de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

2. La Agencia Española de Protección de Datos podrá adherirse a los sistemas de contratación centralizada establecidos por las Administraciones Públicas y participar en la gestión compartida de servicios comunes prevista en el artículo 85 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Disposición adicional vigésima primera. *Educación digital.*

Las Administraciones educativas darán cumplimiento al mandato contenido en el párrafo segundo del apartado 1 del artículo 83 de esta ley orgánica en el plazo de un año a contar desde la entrada en vigor de la misma.

Disposición adicional vigésima segunda. *Acceso a los archivos públicos y eclesiásticos.*

Las autoridades públicas competentes facilitarán el acceso a los archivos públicos y eclesiásticos en relación con los datos que se soliciten con ocasión de investigaciones policiales o judiciales de personas desaparecidas, debiendo atender las solicitudes con prontitud y diligencia las instituciones o congregaciones religiosas a las que se realicen las peticiones de acceso.

Disposición adicional vigésima tercera. *Modelos de presentación de reclamaciones.*

La Agencia Española de Protección de Datos podrá establecer modelos de presentación de reclamaciones ante la misma en todos los ámbitos en los que ésta tenga competencia, que serán de uso obligatorio para los interesados independientemente de que estén obligados o no a relacionarse electrónicamente con las administraciones públicas.

Los modelos serán publicados en el "Boletín Oficial del Estado" y en la Sede Electrónica de la Agencia Española de Protección de Datos y serán de obligado cumplimiento al mes de su publicación en el "Boletín Oficial del Estado".»

Disposición transitoria primera. *Estatuto de la Agencia Española de Protección de Datos.*

1. El Estatuto de la Agencia Española de Protección de Datos, aprobado por Real Decreto 428/1993, de 26 de marzo, continuará vigente en lo que no se oponga a lo establecido en el Título VIII de esta ley orgánica.

2. Lo dispuesto en los apartados 2, 3 y 5 del artículo 48 y en el artículo 49 de esta ley orgánica se aplicará una vez expire el mandato de quien ostente la condición de Director de la Agencia Española de Protección de Datos a la entrada en vigor de la misma.

Disposición transitoria segunda. *Códigos tipo inscritos en las autoridades de protección de datos conforme a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.*

Los promotores de los códigos tipo inscritos en el registro de la Agencia Española de Protección de Datos o en las autoridades autonómicas de protección de datos deberán adaptar su contenido a lo dispuesto en el artículo 40 del Reglamento (UE) 2016/679 en el plazo de un año a contar desde la entrada en vigor de esta ley orgánica.

Si, transcurrido dicho plazo, no se hubiera solicitado la aprobación prevista en el artículo 38.4 de esta ley orgánica, se cancelará la inscripción y se comunicará a sus promotores.

Disposición transitoria tercera. *Régimen transitorio de los procedimientos.*

1. Los procedimientos ya iniciados a la entrada en vigor de esta ley orgánica se regirán por la normativa anterior, salvo que esta ley orgánica contenga disposiciones más favorables para el interesado.

2. Lo dispuesto en el apartado anterior será asimismo de aplicación a los procedimientos respecto de los cuales ya se hubieren iniciado las actuaciones previas a las que se refiere la Sección 2.ª del Capítulo III del Título IX del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, aprobado por Real Decreto 1720/2007, de 21 de diciembre.

Disposición transitoria cuarta. *Tratamientos sometidos a la Directiva (UE) 2016/680.*

Los tratamientos sometidos a la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, continuarán rigiéndose por la Ley Orgánica 15/1999, de 13 de diciembre, y en particular el artículo 22, y sus disposiciones de desarrollo, en tanto no entre en vigor la norma que trasponga al Derecho español lo dispuesto en la citada directiva.

Téngase en cuenta que la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, ha sido transpuesta por la Ley Orgánica 7/2021, de 26 de mayo. Ref. BOE-A-2021-8806

Disposición transitoria quinta. *Contratos de encargado del tratamiento.*

Los contratos de encargado del tratamiento suscritos con anterioridad al 25 de mayo de 2018 al amparo de lo dispuesto en el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal mantendrán su vigencia hasta la fecha de vencimiento señalada en los mismos y en caso de haberse pactado de forma indefinida, hasta el 25 de mayo de 2022.

Durante dichos plazos cualquiera de las partes podrá exigir a la otra la modificación del contrato a fin de que el mismo resulte conforme a lo dispuesto en el artículo 28 del Reglamento (UE) 2016/679 y en el Capítulo II del Título V de esta ley orgánica.

Disposición transitoria sexta. *Reutilización con fines de investigación en materia de salud y biomédica de datos personales recogidos con anterioridad a la entrada en vigor de esta ley orgánica.*

Se considerará lícita y compatible la reutilización con fines de investigación en salud y biomédica de datos personales recogidos lícitamente con anterioridad a la entrada en vigor de esta ley orgánica cuando concurra alguna de las circunstancias siguientes:

a) Que dichos datos personales se utilicen para la finalidad concreta para la que se hubiera prestado consentimiento.

b) Que, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen tales datos para finalidades o áreas de investigación relacionadas con la especialidad médica o investigadora en la que se integrase científicamente el estudio inicial.

Disposición derogatoria única. *Derogación normativa.*

1. Sin perjuicio de lo previsto en la disposición adicional decimocuarta y en la disposición transitoria cuarta, queda derogada la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

2. Queda derogado el Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos.

3. Asimismo, quedan derogadas cuantas disposiciones de igual o inferior rango contradigan, se opongan, o resulten incompatibles con lo dispuesto en el Reglamento (UE) 2016/679 y en la presente ley orgánica.

Disposición final primera. *Naturaleza de la presente ley.*

La presente ley tiene el carácter de ley orgánica.

No obstante, tienen carácter de ley ordinaria:

– El Título IV,
– el Título VII, salvo los artículos 52 y 53, que tienen carácter orgánico,
– el Título VIII,
– el Título IX,
– los artículos 79, 80, 81, 82, 88, 95, 96 y 97 del Título X,
– las disposiciones adicionales, salvo la disposición adicional segunda y la disposición adicional decimoséptima, que tienen carácter orgánico,
– las disposiciones transitorias,
– y las disposiciones finales, salvo las disposiciones finales primera, segunda, tercera, cuarta, octava, décima y decimosexta, que tienen carácter orgánico.

Disposición final segunda. *Título competencial.*

1. Esta ley orgánica se dicta al amparo del artículo 149.1.1.ª de la Constitución, que atribuye al Estado la competencia exclusiva para la regulación de las condiciones básicas que garanticen la igualdad de todos los españoles en el ejercicio de los derechos y en el cumplimiento de los deberes constitucionales.

2. El Capítulo I del Título VII, el Título VIII, la disposición adicional cuarta y la disposición transitoria primera sólo serán de aplicación a la Administración General del Estado y a sus organismos públicos.

3. Los artículos 87 a 90 se dictan al amparo de la competencia exclusiva que el artículo 149.1.7.ª y 18.ª de la Constitución reserva al Estado en materia de legislación laboral y bases del régimen estatutario de los funcionarios públicos respectivamente.

4. La disposición adicional quinta y las disposiciones finales séptima y sexta se dictan al amparo de la competencia que el artículo 149.1.6.ª de la Constitución atribuye al Estado en materia de legislación procesal.

5. La disposición adicional tercera se dicta al amparo del artículo 149.1.18.ª de la Constitución.

6. El artículo 96 se dicta al amparo del artículo 149.1.8.ª de la Constitución.

Disposición final tercera. *Modificación de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General.*

Se modifica la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General que queda redactada como sigue:

Uno. El apartado 3 del artículo treinta y nueve queda redactado como sigue:

> «3. Dentro del plazo anterior, cualquier persona podrá formular reclamación dirigida a la Delegación Provincial de la Oficina del Censo Electoral sobre sus datos censales, si bien solo podrán ser tenidas en cuenta las que se refieran a la rectificación de errores en los datos personales, a los cambios de domicilio dentro de una misma circunscripción o a la no inclusión del reclamante en ninguna Sección del Censo de la circunscripción pese a tener derecho a ello. También serán atendidas las solicitudes de los electores que se opongan a su inclusión en las copias del censo electoral que se faciliten a los representantes de las candidaturas para realizar envíos postales de propaganda electoral. No serán tenidas en cuenta para la elección convocada las que reflejen un cambio de residencia de una circunscripción a otra, realizado con posterioridad a la fecha de cierre del censo para cada elección, debiendo ejercer su derecho en la sección correspondiente a su domicilio anterior.»

Dos. Se añade un nuevo artículo cincuenta y ocho bis, con el contenido siguiente:

> **«Artículo cincuenta y ocho bis.** *Utilización de medios tecnológicos y datos personales en las actividades electorales.*
>
> 1. **(Anulado)**
>
> 2. Los partidos políticos, coaliciones y agrupaciones electorales podrán utilizar datos personales obtenidos en páginas web y otras fuentes de acceso público para la realización de actividades políticas durante el periodo electoral.
>
> 3. El envío de propaganda electoral por medios electrónicos o sistemas de mensajería y la contratación de propaganda electoral en redes sociales o medios equivalentes no tendrán la consideración de actividad o comunicación comercial.
>
> 4. Las actividades divulgativas anteriormente referidas identificarán de modo destacado su naturaleza electoral.
>
> 5. Se facilitará al destinatario un modo sencillo y gratuito de ejercicio del derecho de oposición.»

Disposición final cuarta. *Modificación de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.*

Se modifica la Ley Orgánica, 6/1985, de 1 de julio, del Poder Judicial, en los siguientes términos:

Uno. Se añade un apartado tercero al artículo 58, con la siguiente redacción:

«Artículo 58.

Tercero. De la solicitud de autorización para la declaración prevista en la disposición adicional quinta de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, cuando tal solicitud sea formulada por el Consejo General del Poder Judicial.»

Dos. Se añade una letra f) al artículo 66, con la siguiente redacción:

«Artículo 66.

f) De la solicitud de autorización para la declaración prevista en la disposición adicional quinta de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, cuando tal solicitud sea formulada por la Agencia Española de Protección de Datos.»

Tres. Se añaden una letra k) al apartado 1 y un nuevo apartado 7 al artículo 74, con la siguiente redacción:

«Artículo 74.

1. […]

k) De la solicitud de autorización para la declaración prevista en la disposición adicional quinta de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, cuando tal solicitud sea formulada por la autoridad de protección de datos de la Comunidad Autónoma respectiva.

[…]

7. Corresponde a las Salas de lo Contencioso-administrativo de los Tribunales Superiores de Justicia autorizar, mediante auto, el requerimiento de información por parte de autoridades autonómicas de protección de datos a los operadores que presten servicios de comunicaciones electrónicas disponibles al público y de los prestadores de servicios de la sociedad de la información, cuando ello sea necesario de acuerdo con la legislación específica.»

Cuatro. Se añade un nuevo apartado 7 al artículo 90:

«7. Corresponde a los Juzgados Centrales de lo Contencioso-administrativo autorizar, mediante auto, el requerimiento de información por parte de la Agencia Española de Protección de Datos y otras autoridades administrativas independientes de ámbito estatal a los operadores que presten servicios de comunicaciones electrónicas disponibles al público y de los prestadores de servicios de la sociedad de la información, cuando ello sea necesario de acuerdo con la legislación específica.»

Disposición final quinta. *Modificación de la Ley 14/1986, de 25 de abril, General de Sanidad.*

Se añade un nuevo Capítulo II al Título VI de la Ley 14/1986, de 25 de abril, General de Sanidad con el siguiente contenido:

«CAPÍTULO II

Tratamiento de datos de la investigación en salud

Artículo 105 bis.

El tratamiento de datos personales en la investigación en salud se regirá por lo dispuesto en la Disposición adicional decimoséptima de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales.»

Disposición final sexta. *Modificación de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa.*

La Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, se modifica en los siguientes términos:

Uno. Se añade un nuevo apartado 7 al artículo 10:

«7. Conocerán de la solicitud de autorización al amparo del artículo 122 ter, cuando sea formulada por la autoridad de protección de datos de la Comunidad Autónoma respectiva.»

Dos. Se añade un nuevo apartado 5 al artículo 11:

«5. Conocerá de la solicitud de autorización al amparo del artículo 122 ter, cuando sea formulada por la Agencia Española de Protección de Datos.»

Tres. Se añade un nuevo apartado 4 al artículo 12:

«4. Conocerá de la solicitud de autorización al amparo del artículo 122 ter, cuando sea formulada por el Consejo General del Poder Judicial.»

Cuatro. Se introduce un nuevo artículo 122 ter, con el siguiente tenor:

«Artículo 122 ter. *Procedimiento de autorización judicial de conformidad de una decisión de la Comisión Europea en materia de transferencia internacional de datos.*

1. El procedimiento para obtener la autorización judicial a que se refiere la disposición adicional quinta de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, se iniciará con la solicitud de la autoridad de protección de datos dirigida al Tribunal competente para que se pronuncie acerca de la conformidad de una decisión de la Comisión Europea en materia de transferencia internacional de datos con el Derecho de la Unión Europea. La solicitud irá acompañada de copia del expediente que se encontrase pendiente de resolución ante la autoridad de protección de datos.

2. Serán partes en el procedimiento, además de la autoridad de protección de datos, quienes lo fueran en el procedimiento tramitado ante ella y, en todo caso, la Comisión Europea.

3. El acuerdo de admisión o inadmisión a trámite del procedimiento confirmará, modificará o levantará la suspensión del procedimiento por posible vulneración de la normativa de protección de datos tramitado ante la autoridad de protección de datos, del que trae causa este procedimiento de autorización judicial.

4. Admitida a trámite la solicitud, el Tribunal competente lo notificará a la autoridad de protección de datos a fin de que dé traslado a quienes interviniesen en el procedimiento tramitado ante la misma para que se personen en el plazo de tres días. Igualmente, se dará traslado a la Comisión Europea a los mismos efectos.

5. Concluido el plazo mencionado en la letra anterior, se dará traslado de la solicitud de autorización a las partes personadas a fin de que en el plazo de diez días aleguen lo que estimen procedente, pudiendo solicitar en ese momento la práctica de las pruebas que estimen necesarias.

6. Transcurrido el período de prueba, si alguna de las partes lo hubiese solicitado y el órgano jurisdiccional lo estimase pertinente, se celebrará una vista. El Tribunal

podrá decidir el alcance de las cuestiones sobre las que las partes deberán centrar sus alegaciones en dicha vista.

7. Finalizados los trámites mencionados en los tres apartados anteriores, el Tribunal competente adoptará en el plazo de diez días una de estas decisiones:

a) Si considerase que la decisión de la Comisión Europea es conforme al Derecho de la Unión Europea, dictará sentencia declarándolo así y denegando la autorización solicitada.

b) En caso de considerar que la decisión es contraria al Derecho de la Unión Europea, dictará auto de planteamiento de cuestión prejudicial de validez de la citada decisión ante el Tribunal de Justicia de la Unión Europea, en los términos del artículo 267 del Tratado de Funcionamiento de la Unión Europea.

La autorización solamente podrá ser concedida si la decisión de la Comisión Europea cuestionada fuera declarada inválida por el Tribunal de Justicia de la Unión Europea.

8. El régimen de recursos será el previsto en esta ley.»

Disposición final séptima. *Modificación de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.*

Se modifica el artículo 15 bis de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, que queda redactado como sigue:

«Artículo 15 bis. *Intervención en procesos de defensa de la competencia y de protección de datos.*

1. La Comisión Europea, la Comisión Nacional de los Mercados y la Competencia y los órganos competentes de las comunidades autónomas en el ámbito de sus competencias podrán intervenir en los procesos de defensa de la competencia y de protección de datos, sin tener la condición de parte, por propia iniciativa o a instancia del órgano judicial, mediante la aportación de información o presentación de observaciones escritas sobre cuestiones relativas a la aplicación de los artículos 101 y 102 del Tratado de Funcionamiento de la Unión Europea o los artículos 1 y 2 de la Ley 15/2007, de 3 de julio, de Defensa de la Competencia. Con la venia del correspondiente órgano judicial, podrán presentar también observaciones verbales. A estos efectos, podrán solicitar al órgano jurisdiccional competente que les remita o haga remitir todos los documentos necesarios para realizar una valoración del asunto de que se trate.

La aportación de información no alcanzará a los datos o documentos obtenidos en el ámbito de las circunstancias de aplicación de la exención o reducción del importe de las multas previstas en los artículos 65 y 66 de la Ley 15/2007, de 3 de julio, de Defensa de la Competencia.

2. La Comisión Europea, la Comisión Nacional de los Mercados y la Competencia y los órganos competentes de las comunidades autónomas aportarán la información o presentarán las observaciones previstas en el número anterior diez días antes de la celebración del acto del juicio a que se refiere el artículo 433 o dentro del plazo de oposición o impugnación del recurso interpuesto.

3. Lo dispuesto en los anteriores apartados en materia de procedimiento será asimismo de aplicación cuando la Comisión Europea, la Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos, en el ámbito de sus competencias, consideren precisa su intervención en un proceso que afecte a cuestiones relativas a la aplicación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.»

Disposición final octava. *Modificación de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades.*

Se incluye una nueva letra l) en el apartado 2 del artículo 46 de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, con el contenido siguiente:

«l) La formación en el uso y seguridad de los medios digitales y en la garantía de los derechos fundamentales en Internet.»

Disposición final novena. *Modificación de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.*

Se modifica el apartado 3 del artículo 16 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, que pasa a tener el siguiente tenor:

«Artículo 16. *[…]*

3. El acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, se rige por lo dispuesto en la legislación vigente en materia de protección de datos personales, y en la Ley 14/1986, de 25 de abril, General de Sanidad, y demás normas de aplicación en cada caso. El acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clinicoasistencial, de manera que, como regla general, quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos.

Se exceptúan los supuestos de investigación previstos en el apartado 2 de la Disposición adicional decimoséptima de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales.

Asimismo se exceptúan los supuestos de investigación de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativos con los clinicoasistenciales, en los cuales se estará a lo que dispongan los jueces y tribunales en el proceso correspondiente. El acceso a los datos y documentos de la historia clínica queda limitado estrictamente a los fines específicos de cada caso.

Cuando ello sea necesario para la prevención de un riesgo o peligro grave para la salud de la población, las Administraciones sanitarias a las que se refiere la Ley 33/2011, de 4 de octubre, General de Salud Pública, podrán acceder a los datos identificativos de los pacientes por razones epidemiológicas o de protección de la salud pública. El acceso habrá de realizarse, en todo caso, por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta, asimismo, a una obligación equivalente de secreto, previa motivación por parte de la Administración que solicitase el acceso a los datos.»

Disposición final décima. *Modificación de la Ley Orgánica 2/2006, de 3 de mayo, de Educación.*

Se incluye una nueva letra l) en el apartado 1 del artículo 2 de la Ley Orgánica 2/2006, de 3 de mayo, de Educación, que queda redactado como sigue:

«l) La capacitación para garantizar la plena inserción del alumnado en la sociedad digital y el aprendizaje de un uso seguro de los medios digitales y respetuoso con la dignidad humana, los valores constitucionales, los derechos fundamentales y, particularmente, con el respeto y la garantía de la intimidad individual y colectiva.»

Disposición final undécima. *Modificación de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.*

Se modifica la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, en los siguientes términos:

Uno. Se añade un nuevo artículo 6 bis, con la siguiente redacción:

«Artículo 6 bis. *Registro de actividades de tratamiento.*

Los sujetos enumerados en el artículo 77.1 de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, publicarán su inventario de actividades de tratamiento en aplicación del artículo 31 de la citada Ley Orgánica.»

Dos. El apartado 1 del artículo 15 queda redactado como sigue:

«1. Si la información solicitada contuviera datos personales que revelen la ideología, afiliación sindical, religión o creencias, el acceso únicamente se podrá autorizar en caso de que se contase con el consentimiento expreso y por escrito del afectado, a menos que dicho afectado hubiese hecho manifiestamente públicos los datos con anterioridad a que se solicitase el acceso.

Si la información incluyese datos personales que hagan referencia al origen racial, a la salud o a la vida sexual, incluyese datos genéticos o biométricos o contuviera datos relativos a la comisión de infracciones penales o administrativas que no conllevasen la amonestación pública al infractor, el acceso solo se podrá autorizar en caso de que se cuente con el consentimiento expreso del afectado o si aquel estuviera amparado por una norma con rango de ley.»

Disposición final duodécima. *Modificación de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.*

Se modifican los apartados 2 y 3 del artículo 28 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, que pasan a tener la siguiente redacción:

«Artículo 28. *[…]*

2. Los interesados tienen derecho a no aportar documentos que ya se encuentren en poder de la Administración actuante o hayan sido elaborados por cualquier otra Administración. La administración actuante podrá consultar o recabar dichos documentos salvo que el interesado se opusiera a ello. No cabrá la oposición cuando la aportación del documento se exigiera en el marco del ejercicio de potestades sancionadoras o de inspección.

Las Administraciones Públicas deberán recabar los documentos electrónicamente a través de sus redes corporativas o mediante consulta a las plataformas de intermediación de datos u otros sistemas electrónicos habilitados al efecto.

Cuando se trate de informes preceptivos ya elaborados por un órgano administrativo distinto al que tramita el procedimiento, estos deberán ser remitidos en el plazo de diez días a contar desde su solicitud. Cumplido este plazo, se informará al interesado de que puede aportar este informe o esperar a su remisión por el órgano competente.

3. Las Administraciones no exigirán a los interesados la presentación de documentos originales, salvo que, con carácter excepcional, la normativa reguladora aplicable establezca lo contrario.

Asimismo, las Administraciones Públicas no requerirán a los interesados datos o documentos no exigidos por la normativa reguladora aplicable o que hayan sido aportados anteriormente por el interesado a cualquier Administración. A estos efectos, el interesado deberá indicar en qué momento y ante qué órgano administrativo presentó los citados documentos, debiendo las Administraciones Públicas recabarlos electrónicamente a través de sus redes corporativas o de una consulta a las plataformas de intermediación de datos u otros sistemas electrónicos habilitados al efecto, salvo que conste en el procedimiento la oposición expresa del interesado o la ley especial aplicable requiera su consentimiento expreso. Excepcionalmente, si las Administraciones Públicas no pudieran recabar los citados documentos, podrán solicitar nuevamente al interesado su aportación.»

Disposición final decimotercera. *Modificación del texto refundido de la Ley del Estatuto de los Trabajadores.*

Se añade un nuevo artículo 20 bis al texto refundido de la Ley del Estatuto de los Trabajadores, aprobado por Real Decreto Legislativo 2/2015, de 23 de octubre, con el siguiente contenido:

> **«Artículo 20 bis.** *Derechos de los trabajadores a la intimidad en relación con el entorno digital y a la desconexión.*
>
> Los trabajadores tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador, a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales.»

Disposición final decimocuarta. *Modificación del texto refundido de la Ley del Estatuto Básico del Empleado Público.*

Se añade una nueva letra j bis) en el artículo 14 del texto refundido de la Ley del Estatuto Básico del Empleado Público, aprobado por Real Decreto Legislativo 5/2015, de 30 de octubre, que quedará redactada como sigue:

> «j bis) A la intimidad en el uso de dispositivos digitales puestos a su disposición y frente al uso de dispositivos de videovigilancia y geolocalización, así como a la desconexión digital en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales.»

Disposición final decimoquinta. *Desarrollo normativo.*

Se habilita al Gobierno para desarrollar lo dispuesto en los artículos 3.2, 38.6, 45.2, 63.3, 96.3 y disposición adicional sexta, en los términos establecidos en ellos.

Disposición final decimosexta. *Entrada en vigor.*

La presente ley orgánica entrará en vigor el día siguiente al de su publicación en el Boletín Oficial del Estado.

§ 52

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal

Ministerio de Justicia
«BOE» núm. 17, de 19 de enero de 2008
Última modificación: 8 de marzo de 2012
Referencia: BOE-A-2008-979

La actual Ley Orgánica 15/1999, de 13 de diciembre de Protección de datos de carácter personal adaptó nuestro ordenamiento a lo dispuesto por la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, derogando a su vez la hasta entonces vigente Ley Orgánica 5/1992, de 29 de octubre, de Regulación del tratamiento automatizado de datos de carácter personal.

La nueva ley, que ha nacido con una amplia vocación de generalidad, prevé en su artículo 1 que «tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal». Comprende por tanto el tratamiento automatizado y el no automatizado de los datos de carácter personal.

A fin de garantizar la necesaria seguridad jurídica en un ámbito tan sensible para los derechos fundamentales como el de la protección de datos, el legislador declaró subsistentes las normas reglamentarias existentes y, en especial, los reales decretos 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos, 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre de Regulación del tratamiento automatizado de los datos de carácter personal y 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, a la vez que habilitó al Gobierno para la aprobación o modificación de las disposiciones reglamentarias necesarias para la aplicación y desarrollo de la Ley Orgánica 15/1999.

Por otra parte, la Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico y la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones atribuyen competencias en materia sancionadora a la Agencia Española de Protección de Datos. Éstas requieren de desarrollo reglamentario con la peculiaridad de que ambas normas se ordenan a la tutela no sólo de los derechos de las personas físicas, sino también de las jurídicas.

II

Este Reglamento comparte con la Ley Orgánica la finalidad de hacer frente a los riesgos que para los derechos de la personalidad pueden suponer el acopio y tratamiento de datos personales. Por ello, ha de destacarse que esta norma reglamentaria nace con la vocación de no reiterar los contenidos de la norma superior y de desarrollar, no sólo los mandatos contenidos en la Ley Orgánica de acuerdo con los principios que emanan de la Directiva, sino también aquellos que en estos años de vigencia de la Ley se ha demostrado que precisan de un mayor desarrollo normativo.

Por tanto, se aprueba este Reglamento partiendo de la necesidad de dotar de coherencia a la regulación reglamentaria en todo lo relacionado con la transposición de la Directiva y de desarrollar los aspectos novedosos de la Ley Orgánica 15/1999, junto con aquellos en los que la experiencia ha aconsejado un cierto de grado de precisión que dote de seguridad jurídica al sistema.

III

El reglamento viene a abarcar el ámbito tutelado anteriormente por los reales decretos 1332/1994, de 20 de junio, y 994/1999, de 11 de junio, teniendo en cuenta la necesidad de fijar criterios aplicables a los ficheros y tratamientos de datos personales no automatizados. Por otra parte, la atribución de funciones a la Agencia Española de Protección de Datos por la Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico y la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones obliga a desarrollar también los procedimientos para el ejercicio de la potestad sancionadora por la Agencia.

El reglamento se estructura en nueve títulos cuyo contenido desarrolla los aspectos esenciales en esta materia.

El título I contempla el objeto y ámbito de aplicación del reglamento. A lo largo de la vigencia de la Ley Orgánica 15/1999, se ha advertido la conveniencia de desarrollar el apartado 2 de su artículo 2 para aclarar qué se entiende por ficheros y tratamientos relacionados con actividades personales o domésticas, aspecto muy relevante dado que están excluidos de la normativa sobre protección de datos de carácter personal.

Por otra parte, el presente reglamento no contiene previsiones para los tratamientos de datos personales a los que se refiere el apartado 3 del artículo 2 de la ley orgánica, dado que se rigen por sus disposiciones específicas y por lo especialmente previsto, en su caso, por la propia Ley Orgánica 15/1999. En consecuencia, se mantiene el régimen jurídico propio de estos tratamientos y ficheros.

Además, en este título se aporta un conjunto de definiciones que ayudan al correcto entendimiento de la norma, lo que resulta particularmente necesario en un ámbito tan tecnificado como el de la protección de datos personales. Por otra parte, fija el criterio a seguir en materia de cómputo de plazos con el fin de homogeneizar esta cuestión evitando distinciones que suponen diferencias de trato de los ficheros públicos respecto de los privados.

El título II, se refiere a los principios de la protección de datos. Reviste particular importancia la regulación del modo de captación del consentimiento atendiendo a aspectos muy específicos como el caso de los servicios de comunicaciones electrónicas y, muy particularmente, la captación de datos de los menores. Asimismo, se ofrece lo que no puede definirse sino como un estatuto del encargado del tratamiento, que sin duda contribuirá a clarificar todo lo relacionado con esta figura. Las previsiones en este ámbito se completan con lo dispuesto en el título VIII en materia de seguridad dotando de un marco coherente a la actuación del encargado.

El título III se ocupa de una cuestión tan esencial como los derechos de las personas en este ámbito. Estos derechos de acceso, rectificación, cancelación y oposición al tratamiento, según ha afirmado el Tribunal Constitucional en su sentencia número 292/2000, constituyen el haz de facultades que emanan del derecho fundamental a la protección de datos y «sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer».

A continuación, los títulos IV a VII permiten clarificar aspectos importantes para el tráfico ordinario, como la aplicación de criterios específicos a determinado tipo de ficheros de titularidad privada que por su trascendencia lo requerían -los relativos a la solvencia patrimonial y crédito y los utilizados en actividades de publicidad y prospección comercial-, el conjunto de obligaciones materiales y formales que deben conducir a los responsables a la creación e inscripción de los ficheros, los criterios y procedimientos para la realización de las transferencias internacionales de datos, y, finalmente, la regulación de un instrumento, el código tipo, llamado a jugar cada vez un papel más relevante como elemento dinamizador del derecho fundamental a la protección de datos.

El título VIII regula un aspecto esencial para la tutela del derecho fundamental a la protección de datos, la seguridad, que repercute sobre múltiples aspectos organizativos, de gestión y aún de inversión, en todas las organizaciones que traten datos personales. La repercusión del deber de seguridad obligaba a un particular rigor ya que en esta materia han confluido distintos elementos muy relevantes. Por una parte, la experiencia dimanante de la aplicación del Real Decreto 994/1999 permitía conocer las dificultades que habían enfrentado los responsables e identificar los puntos débiles y fuertes de la regulación. Por otra, se reclamaba la adaptación de la regulación en distintos aspectos. En este sentido, el reglamento trata de ser particularmente riguroso en la atribución de los niveles de seguridad, en la fijación de las medidas que corresponda adoptar en cada caso y en la revisión de las mismas cuando ello resulte necesario. Por otra parte, ordena con mayor precisión el contenido y las obligaciones vinculadas al mantenimiento del documento de seguridad. Además, se ha pretendido regular la materia de modo que contemple las múltiples formas de organización material y personal de la seguridad que se dan en la práctica. Por último, se regula un conjunto de medidas destinadas a los ficheros y tratamientos estructurados y no automatizados que ofrezca a los responsables un marco claro de actuación.

Finalmente en el título IX, dedicado a los procedimientos tramitados por la Agencia Española de Protección de Datos, se ha optado por normar exclusivamente aquellas especialidades que diferencian a los distintos procedimientos tramitados por la Agencia de las normas generales previstas para los procedimientos en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, cuya aplicación se declara supletoria al presente reglamento.

En su virtud, a propuesta del Ministro de Justicia, con la aprobación previa de la Ministra de Administraciones Públicas, de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros en su reunión del día 21 de diciembre de 2007.

D I S P O N G O :

Artículo único. *Aprobación del reglamento.*

Se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal, cuyo texto se incluye a continuación.

Disposición transitoria primera. *Adaptación de los códigos tipo inscritos en el Registro General de Protección de Datos.*

En el plazo de un año desde la entrada en vigor del presente real decreto deberán notificarse a la Agencia Española de Protección de Datos las modificaciones que resulten necesarias en los códigos tipo inscritos en el Registro General de Protección de Datos para adaptar su contenido a lo dispuesto en el título VII del mismo.

Disposición transitoria segunda. *Plazos de implantación de las medidas de seguridad.*

La implantación de las medidas de seguridad previstas en el presente real decreto deberá producirse con arreglo a las siguientes reglas:

1.ª Respecto de los ficheros automatizados que existieran en la fecha de entrada en vigor del presente real decreto:

a) En el plazo de un año desde su entrada en vigor, deberán implantarse las medidas de seguridad de nivel medio exigibles a los siguientes ficheros:

1.º Aquéllos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias.

2.º Aquéllos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.

3.º Aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos, respecto de las medidas de este nivel que no fueran exigibles conforme a lo previsto en el artículo 4.4 del Reglamento de Medidas de seguridad de los ficheros automatizados de datos de carácter personal, aprobado por Real Decreto 994/1999, de 11 de junio.

b) En el plazo de un año desde su entrada en vigor deberán implantarse las medidas de seguridad de nivel medio y en el de dieciocho meses desde aquella fecha, las de nivel alto exigibles a los siguientes ficheros:

1.º Aquéllos que contengan datos derivados de actos de violencia de género.

2.º Aquéllos de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización.

c) En los demás supuestos, cuando el presente reglamento exija la implantación de una medida adicional, no prevista en el Reglamento de Medidas de seguridad de los ficheros automatizados de datos de carácter personal, aprobado por Real Decreto 994/1999, de 11 de junio, dicha medida deberá implantarse en el plazo de un año desde la entrada en vigor del presente real decreto.

2.ª Respecto de los ficheros no automatizados que existieran en la fecha de entrada en vigor del presente real decreto:

a) Las medidas de seguridad de nivel básico deberán implantarse en el plazo de un año desde su entrada en vigor.

b) Las medidas de seguridad de nivel medio deberán implantarse en el plazo de dieciocho meses desde su entrada en vigor.

c) Las medidas de seguridad de nivel alto deberán implantarse en el plazo de dos años desde su entrada en vigor.

3.ª Los ficheros, tanto automatizados como no automatizados, creados con posterioridad a la fecha de entrada en vigor del presente real decreto deberán tener implantadas, desde el momento de su creación la totalidad de las medidas de seguridad reguladas en el mismo.

Disposición transitoria tercera. *Régimen transitorio de las solicitudes para el ejercicio de los derechos de las personas.*

A las solicitudes para el ejercicio de los derechos de acceso, oposición, rectificación y cancelación que hayan sido efectuadas antes de la entrada en vigor del presente real decreto, no les será de aplicación el mismo, rigiéndose por la normativa anterior.

Disposición transitoria cuarta. *Régimen transitorio de los procedimientos.*

A los procedimientos ya iniciados antes de la entrada en vigor del presente real decreto, no les será de aplicación el mismo, rigiéndose por la normativa anterior.

Disposición transitoria quinta. *Régimen transitorio de las actuaciones previas.*

A las actuaciones previas iniciadas con anterioridad a la entrada en vigor del presente real decreto, no les será de aplicación el mismo, rigiéndose por la normativa anterior.

El presente real decreto se aplicará a las actuaciones previas que se inicien después de su entrada en vigor.

Disposición derogatoria única. *Derogación normativa.*

Quedan derogados el Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del

tratamiento automatizado de los datos de carácter personal, el Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal y todas las normas de igual o inferior rango que contradigan o se opongan a lo dispuesto en el presente real decreto.

Disposición final primera. *Título competencial.*

El título I, con excepción del apartado c) del artículo 4, los títulos II, III, VII y VIII, así como los artículos 52, 53.3, 53.4, 54, 55.1, 55.3, 56, 57, 58 y 63.3 del reglamento se dictan al amparo de lo dispuesto en el artículo 149.1.1.ª de la Constitución, que atribuye al Estado la competencia exclusiva para la regulación de las condiciones básicas que garanticen la igualdad de todos los españoles en el ejercicio de los derechos y en el cumplimiento de los deberes constitucionales.

Disposición final segunda. *Entrada en vigor.*

El presente real decreto entrará en vigor a los tres meses de su íntegra publicación en el «Boletín Oficial del Estado».

REGLAMENTO DE DESARROLLO DE LA LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE, DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

TÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

1. El presente reglamento tiene por objeto el desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal.

2. Asimismo, el capítulo III del título IX de este reglamento desarrolla las disposiciones relativas al ejercicio por la Agencia Española de Protección de Datos de la potestad sancionadora, en aplicación de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, en el título VII de la Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico, y en el título VIII de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

Artículo 2. *Ámbito objetivo de aplicación.*

1. El presente reglamento será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.

2. Este reglamento no será aplicable a los tratamientos de datos referidos a personas jurídicas, ni a los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales.

3. Asimismo, los datos relativos a empresarios individuales, cuando hagan referencia a ellos en su calidad de comerciantes, industriales o navieros, también se entenderán excluidos del régimen de aplicación de la protección de datos de carácter personal.

4. Este reglamento no será de aplicación a los datos referidos a personas fallecidas. No obstante, las personas vinculadas al fallecido, por razones familiares o análogas, podrán dirigirse a los responsables de los ficheros o tratamientos que contengan datos de éste con la finalidad de notificar el óbito, aportando acreditación suficiente del mismo, y solicitar, cuando hubiere lugar a ello, la cancelación de los datos.

Artículo 3. *Ámbito territorial de aplicación.*

1. Se regirá por el presente reglamento todo tratamiento de datos de carácter personal:

a) Cuando el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento, siempre que dicho establecimiento se encuentre ubicado en territorio español.

Cuando no resulte de aplicación lo dispuesto en el párrafo anterior, pero exista un encargado del tratamiento ubicado en España, serán de aplicación al mismo las normas contenidas en el título VIII del presente reglamento.

b) Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española, según las normas de Derecho internacional público.

c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.

En este supuesto, el responsable del tratamiento deberá designar un representante establecido en territorio español.

2. A los efectos previstos en los apartados anteriores, se entenderá por establecimiento, con independencia de su forma jurídica, cualquier instalación estable que permita el ejercicio efectivo y real de una actividad.

Artículo 4. *Ficheros o tratamientos excluidos.*

El régimen de protección de los datos de carácter personal que se establece en el presente reglamento no será de aplicación a los siguientes ficheros y tratamientos:

a) A los realizados o mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.

Sólo se considerarán relacionados con actividades personales o domésticas los tratamientos relativos a las actividades que se inscriben en el marco de la vida privada o familiar de los particulares.

b) A los sometidos a la normativa sobre protección de materias clasificadas.

c) A los establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia Española de Protección de Datos.

Artículo 5. *Definiciones.*

1. A los efectos previstos en este reglamento, se entenderá por:

a) Afectado o interesado: Persona física titular de los datos que sean objeto del tratamiento.

b) Cancelación: Procedimiento en virtud del cual el responsable cesa en el uso de los datos. La cancelación implicará el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos.

c) Cesión o comunicación de datos: Tratamiento de datos que supone su revelación a una persona distinta del interesado.

d) Consentimiento del interesado: Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

e) Dato disociado: aquél que no permite la identificación de un afectado o interesado.

f) Datos de carácter personal: Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.

g) Datos de carácter personal relacionados con la salud: las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética.

h) Destinatario o cesionario: la persona física o jurídica, pública o privada u órgano administrativo, al que se revelen los datos.

Podrán ser también destinatarios los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

i) Encargado del tratamiento: La persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

Podrán ser también encargados del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

j) Exportador de datos personales: la persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realice, conforme a lo dispuesto en el presente Reglamento, una transferencia de datos de carácter personal a un país tercero.

k) Fichero: Todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

l) Ficheros de titularidad privada: los ficheros de los que sean responsables las personas, empresas o entidades de derecho privado, con independencia de quien ostente la titularidad de su capital o de la procedencia de sus recursos económicos, así como los ficheros de los que sean responsables las corporaciones de derecho público, en cuanto dichos ficheros no se encuentren estrictamente vinculados al ejercicio de potestades de derecho público que a las mismas atribuye su normativa específica.

m) Ficheros de titularidad pública: los ficheros de los que sean responsables los órganos constitucionales o con relevancia constitucional del Estado o las instituciones autonómicas con funciones análogas a los mismos, las Administraciones públicas territoriales, así como las entidades u organismos vinculados o dependientes de las mismas y las Corporaciones de derecho público siempre que su finalidad sea el ejercicio de potestades de derecho público.

n) Fichero no automatizado: todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica.

ñ) Importador de datos personales: la persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos en caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargada del tratamiento o tercero.

o) Persona identificable: toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados.

p) Procedimiento de disociación: Todo tratamiento de datos personales que permita la obtención de datos disociados.

q) Responsable del fichero o del tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.

Podrán ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

r) Tercero: la persona física o jurídica, pública o privada u órgano administrativo distinta del afectado o interesado, del responsable del tratamiento, del responsable del fichero, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento.

Podrán ser también terceros los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

s) Transferencia internacional de datos: Tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien

constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español.

t) Tratamiento de datos: cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, modificación, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

2. En particular, en relación con lo dispuesto en el título VIII de este reglamento se entenderá por:

a) Accesos autorizados: autorizaciones concedidas a un usuario para la utilización de los diversos recursos. En su caso, incluirán las autorizaciones o funciones que tenga atribuidas un usuario por delegación del responsable del fichero o tratamiento o del responsable de seguridad.

b) Autenticación: procedimiento de comprobación de la identidad de un usuario.

c) Contraseña: información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario o en el acceso a un recurso.

d) Control de acceso: mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.

e) Copia de respaldo: copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.

f) Documento: todo escrito, gráfico, sonido, imagen o cualquier otra clase de información que puede ser tratada en un sistema de información como una unidad diferenciada.

g) Ficheros temporales: ficheros de trabajo creados por usuarios o procesos que son necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento.

h) Identificación: procedimiento de reconocimiento de la identidad de un usuario.

i) Incidencia: cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

j) Perfil de usuario: accesos autorizados a un grupo de usuarios.

k) Recurso: cualquier parte componente de un sistema de información.

l) Responsable de seguridad: persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

m) Sistema de información: conjunto de ficheros, tratamientos, programas, soportes y en su caso, equipos empleados para el tratamiento de datos de carácter personal.

n) Sistema de tratamiento: modo en que se organiza o utiliza un sistema de información. Atendiendo al sistema de tratamiento, los sistemas de información podrán ser automatizados, no automatizados o parcialmente automatizados.

ñ) Soporte: objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos.

o) Transmisión de documentos: cualquier traslado, comunicación, envío, entrega o divulgación de la información contenida en el mismo.

p) Usuario: sujeto o proceso autorizado para acceder a datos o recursos. Tendrán la consideración de usuarios los procesos que permitan acceder a datos o recursos sin identificación de un usuario físico.

Artículo 6. *Cómputo de plazos.*

En los supuestos en que este reglamento señale un plazo por días se computarán únicamente los hábiles. Cuando el plazo sea por meses, se computarán de fecha a fecha.

Artículo 7. *Fuentes accesibles al público.*

1. A efectos del artículo 3, párrafo j) de la Ley Orgánica 15/1999, se entenderá que sólo tendrán el carácter de fuentes accesibles al público:

a) El censo promocional, regulado conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre.

b) Las guías de servicios de comunicaciones electrónicas, en los términos previstos por su normativa específica.

c) Las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección profesional e indicación de su pertenencia al grupo. La dirección profesional podrá incluir los datos del domicilio postal completo, número telefónico, número de fax y dirección electrónica. En el caso de Colegios profesionales, podrán indicarse como datos de pertenencia al grupo los de número de colegiado, fecha de incorporación y situación de ejercicio profesional.

d) Los diarios y boletines oficiales.

e) Los medios de comunicación social.

2. En todo caso, para que los supuestos enumerados en el apartado anterior puedan ser considerados fuentes accesibles al público, será preciso que su consulta pueda ser realizada por cualquier persona, no impedida por una norma limitativa, o sin más exigencia que, en su caso, el abono de una contraprestación.

TÍTULO II

Principios de protección de datos

CAPÍTULO I

Calidad de los datos

Artículo 8. *Principios relativos a la calidad de los datos.*

1. Los datos de carácter personal deberán ser tratados de forma leal y lícita. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

2. Los datos de carácter personal sólo podrán ser recogidos para el cumplimiento de finalidades determinadas, explícitas y legítimas del responsable del tratamiento.

3. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos.

4. Sólo podrán ser objeto de tratamiento los datos que sean adecuados, pertinentes y no excesivos en relación con las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

5. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado. Si los datos fueran recogidos directamente del afectado, se considerarán exactos los facilitados por éste.

Si los datos de carácter personal sometidos a tratamiento resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados en el plazo de diez días desde que se tuviese conocimiento de la inexactitud, salvo que la legislación aplicable al fichero establezca un procedimiento o un plazo específico para ello.

Cuando los datos hubieran sido comunicados previamente, el responsable del fichero o tratamiento deberá notificar al cesionario, en el plazo de diez días, la rectificación o cancelación efectuada, siempre que el cesionario sea conocido.

En el plazo de diez días desde la recepción de la notificación, el cesionario que mantuviera el tratamiento de los datos, deberá proceder a la rectificación y cancelación notificada.

Esta actualización de los datos de carácter personal no requerirá comunicación alguna al interesado, sin perjuicio del ejercicio de los derechos por parte de los interesados reconocidos en la Ley Orgánica 15/1999, de 13 de diciembre.

Lo dispuesto en este apartado se entiende sin perjuicio de las facultades que a los afectados reconoce el título III de este reglamento.

6. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

No obstante, podrán conservarse durante el tiempo en que pueda exigirse algún tipo de responsabilidad derivada de una relación u obligación jurídica o de la ejecución de un contrato o de la aplicación de medidas precontractuales solicitadas por el interesado.

Una vez cumplido el período al que se refieren los párrafos anteriores, los datos sólo podrán ser conservados previa disociación de los mismos, sin perjuicio de la obligación de bloqueo prevista en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente reglamento.

7. Los datos de carácter personal serán tratados de forma que permitan el ejercicio del derecho de acceso, en tanto no proceda su cancelación.

Artículo 9. *Tratamiento con fines estadísticos, históricos o científicos.*

1. No se considerará incompatible, a los efectos previstos en el apartado 3 del artículo anterior, el tratamiento de los datos de carácter personal con fines históricos, estadísticos o científicos.

Para la determinación de los fines a los que se refiere el párrafo anterior se estará a la legislación que en cada caso resulte aplicable y, en particular, a lo dispuesto en la Ley 12/1989, de 9 de mayo, Reguladora de la función estadística pública, la Ley 16/1985, de 25 junio, del Patrimonio histórico español y la Ley 13/1986, de 14 de abril de Fomento y coordinación general de la investigación científica y técnica, y sus respectivas disposiciones de desarrollo, así como a la normativa autonómica en estas materias.

2. Por vía de excepción a lo dispuesto en el apartado 6 del artículo anterior, la Agencia Española de Protección de Datos o, en su caso, las autoridades de control de las comunidades autónomas podrán, previa solicitud del responsable del tratamiento y conforme al procedimiento establecido en la sección segunda del capítulo VII del título IX del presente reglamento, acordar el mantenimiento íntegro de determinados datos, atendidos sus valores históricos, estadísticos o científicos de acuerdo con las normas a las que se refiere el apartado anterior.

Artículo 10. *Supuestos que legitiman el tratamiento o cesión de los datos.*

1. Los datos de carácter personal únicamente podrán ser objeto de tratamiento o cesión si el interesado hubiera prestado previamente su consentimiento para ello.

2. No obstante, será posible el tratamiento o la cesión de los datos de carácter personal sin necesidad del consentimiento del interesado cuando:

a) Lo autorice una norma con rango de ley o una norma de derecho comunitario y, en particular, cuando concurra uno de los supuestos siguientes:

El tratamiento o la cesión tengan por objeto la satisfacción de un interés legítimo del responsable del tratamiento o del cesionario amparado por dichas normas, siempre que no prevalezca el interés o los derechos y libertades fundamentales de los interesados previstos en el artículo 1 de la Ley Orgánica 15/1999, de 13 de diciembre.

El tratamiento o la cesión de los datos sean necesarios para que el responsable del tratamiento cumpla un deber que le imponga una de dichas normas.

b) **(Anulado)**

3. Los datos de carácter personal podrán tratarse sin necesidad del consentimiento del interesado cuando:

a) Se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de las competencias que les atribuya una norma con rango de ley o una norma de derecho comunitario.

b) Se recaben por el responsable del tratamiento con ocasión de la celebración de un contrato o precontrato o de la existencia de una relación negocial, laboral o administrativa de la que sea parte el afectado y sean necesarios para su mantenimiento o cumplimiento.

c) El tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del apartado 6 del artículo 7 de la Ley Orgánica 15/1999, de 13 de diciembre.

4. Será posible la cesión de los datos de carácter personal sin contar con el consentimiento del interesado cuando:

a) La cesión responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control comporte la comunicación de los datos. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

b) La comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas o a las instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas y se realice en el ámbito de las funciones que la ley les atribuya expresamente.

c) La cesión entre Administraciones públicas cuando concurra uno de los siguientes supuestos:

Tenga por objeto el tratamiento de los datos con fines históricos, estadísticos o científicos.

Los datos de carácter personal hayan sido recogidos o elaborados por una Administración pública con destino a otra.

La comunicación se realice para el ejercicio de competencias idénticas o que versen sobre las mismas materias.

5. Los datos especialmente protegidos podrán tratarse y cederse en los términos previstos en los artículos 7 y 8 de la Ley Orgánica 15/1999, de 13 de diciembre.

En particular, no será necesario el consentimiento del interesado para la comunicación de datos personales sobre la salud, incluso a través de medios electrónicos, entre organismos, centros y servicios del Sistema Nacional de Salud cuando se realice para la atención sanitaria de las personas, conforme a lo dispuesto en el Capítulo V de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.

Artículo 11. *Verificación de datos en solicitudes formuladas a las Administraciones públicas.*

(Anulado)

CAPÍTULO II

Consentimiento para el tratamiento de los datos y deber de información

Sección 1.ª Obtención del consentimiento del afectado

Artículo 12. *Principios generales.*

1. El responsable del tratamiento deberá obtener el consentimiento del interesado para el tratamiento de sus datos de carácter personal salvo en aquellos supuestos en que el mismo no sea exigible con arreglo a lo dispuesto en las leyes.

La solicitud del consentimiento deberá ir referida a un tratamiento o serie de tratamientos concretos, con delimitación de la finalidad para los que se recaba, así como de las restantes condiciones que concurran en el tratamiento o serie de tratamientos.

2. Cuando se solicite el consentimiento del afectado para la cesión de sus datos, éste deberá ser informado de forma que conozca inequívocamente la finalidad a la que se destinarán los datos respecto de cuya comunicación se solicita el consentimiento y el tipo de actividad desarrollada por el cesionario. En caso contrario, el consentimiento será nulo.

3. Corresponderá al responsable del tratamiento la prueba de la existencia del consentimiento del afectado por cualquier medio de prueba admisible en derecho.

Artículo 13. *Consentimiento para el tratamiento de datos de menores de edad.*

1. Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores.

2. En ningún caso podrán recabarse del menor datos que permitan obtener información sobre los demás miembros del grupo familiar, o sobre las características del mismo, como los datos relativos a la actividad profesional de los progenitores, información económica, datos sociológicos o cualesquiera otros, sin el consentimiento de los titulares de tales datos.

No obstante, podrán recabarse los datos de identidad y dirección del padre, madre o tutor con la única finalidad de recabar la autorización prevista en el apartado anterior.

3. Cuando el tratamiento se refiera a datos de menores de edad, la información dirigida a los mismos deberá expresarse en un lenguaje que sea fácilmente comprensible por aquéllos, con expresa indicación de lo dispuesto en este artículo.

4. Corresponderá al responsable del fichero o tratamiento articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado en su caso, por los padres, tutores o representantes legales.

Artículo 14. *Forma de recabar el consentimiento.*

1. El responsable del tratamiento podrá solicitar el consentimiento del interesado a través del procedimiento establecido en este artículo, salvo cuando la Ley exija al mismo la obtención del consentimiento expreso para el tratamiento de los datos.

2. El responsable podrá dirigirse al afectado, informándole en los términos previstos en los artículos 5 de la Ley Orgánica 15/1999, de 13 de diciembre y 12.2 de este reglamento y deberá concederle un plazo de treinta días para manifestar su negativa al tratamiento, advirtiéndole de que en caso de no pronunciarse a tal efecto se entenderá que consiente el tratamiento de sus datos de carácter personal.

En particular, cuando se trate de responsables que presten al afectado un servicio que genere información periódica o reiterada, o facturación periódica, la comunicación podrá llevarse a cabo de forma conjunta a esta información o a la facturación del servicio prestado, siempre que se realice de forma claramente visible.

3. En todo caso, será necesario que el responsable del tratamiento pueda conocer si la comunicación ha sido objeto de devolución por cualquier causa, en cuyo caso no podrá proceder al tratamiento de los datos referidos a ese interesado.

4. Deberá facilitarse al interesado un medio sencillo y gratuito para manifestar su negativa al tratamiento de los datos. En particular, se considerará ajustado al presente reglamento los procedimientos en el que tal negativa pueda efectuarse, entre otros, mediante un envío prefranqueado al responsable del tratamiento, la llamada a un número telefónico gratuito o a los servicios de atención al público que el mismo hubiera establecido.

5. Cuando se solicite el consentimiento del interesado a través del procedimiento establecido en este artículo, no será posible solicitarlo nuevamente respecto de los mismos tratamientos y para las mismas finalidades en el plazo de un año a contar de la fecha de la anterior solicitud.

Artículo 15. *Solicitud del consentimiento en el marco de una relación contractual para fines no relacionados directamente con la misma.*

Si el responsable del tratamiento solicitase el consentimiento del afectado durante el proceso de formación de un contrato para finalidades que no guarden relación directa con el mantenimiento, desarrollo o control de la relación contractual, deberá permitir al afectado que manifieste expresamente su negativa al tratamiento o comunicación de datos.

En particular, se entenderá cumplido tal deber cuando se permita al afectado la marcación de una casilla claramente visible y que no se encuentre ya marcada en el documento que se le entregue para la celebración del contrato o se establezca un procedimiento equivalente que le permita manifestar su negativa al tratamiento.

Artículo 16. *Tratamiento de datos de facturación y tráfico en servicios de comunicaciones electrónicas.*

La solicitud del consentimiento para el tratamiento o cesión de los datos de tráfico, facturación y localización por parte de los sujetos obligados, o en su caso la revocación de aquél, según la legislación reguladora de las telecomunicaciones se someterá a lo establecido en su normativa específica y, en lo que no resulte contrario a la misma, a lo establecido en la presente sección.

Artículo 17. *Revocación del consentimiento.*

1. El afectado podrá revocar su consentimiento a través de un medio sencillo, gratuito y que no implique ingreso alguno para el responsable del fichero o tratamiento. En particular, se considerará ajustado al presente reglamento el procedimiento en el que tal negativa pueda efectuarse, entre otros, mediante un envío prefranqueado al responsable del tratamiento o la llamada a un número telefónico gratuito o a los servicios de atención al público que el mismo hubiera establecido.

No se considerarán conformes a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, los supuestos en que el responsable establezca como medio para que el interesado pueda manifestar su negativa al tratamiento el envío de cartas certificadas o envíos semejantes, la utilización de servicios de telecomunicaciones que implique una tarificación adicional al afectado o cualesquiera otros medios que impliquen un coste adicional al interesado.

2. El responsable cesará en el tratamiento de los datos en el plazo máximo de diez días a contar desde el de la recepción de la revocación del consentimiento, sin perjuicio de su obligación de bloquear los datos conforme a lo dispuesto en el artículo 16.3 de la Ley Orgánica 15/1999, de 13 de diciembre.

3. Cuando el interesado hubiera solicitado del responsable del tratamiento la confirmación del cese en el tratamiento de sus datos, éste deberá responder expresamente a la solicitud.

4. Si los datos hubieran sido cedidos previamente, el responsable del tratamiento, una vez revocado el consentimiento, deberá comunicarlo a los cesionarios, en el plazo previsto en el apartado 2, para que éstos, cesen en el tratamiento de los datos en caso de que aún lo mantuvieran, conforme al artículo 16.4 de la Ley Orgánica 15/1999, de 13 de diciembre.

Sección 2.ª Deber de información al interesado

Artículo 18. *Acreditación del cumplimiento del deber de información.*

(Anulado)

Artículo 19. *Supuestos especiales.*

En los supuestos en que se produzca una modificación del responsable del fichero como consecuencia de una operación de fusión, escisión, cesión global de activos y pasivos, aportación o transmisión de negocio o rama de actividad empresarial, o cualquier operación de reestructuración societaria de análoga naturaleza, contemplada por la normativa mercantil, no se producirá cesión de datos, sin perjuicio del cumplimiento por el responsable de lo dispuesto en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre.

CAPÍTULO III

Encargado del tratamiento

Artículo 20. *Relaciones entre el responsable y el encargado del tratamiento.*

1. El acceso a los datos por parte de un encargado del tratamiento que resulte necesario para la prestación de un servicio al responsable no se considerará comunicación de datos, siempre y cuando se cumpla lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre y en el presente capítulo.

El servicio prestado por el encargado del tratamiento podrá tener o no carácter remunerado y ser temporal o indefinido.

No obstante, se considerará que existe comunicación de datos cuando el acceso tenga por objeto el establecimiento de un nuevo vínculo entre quien accede a los datos y el afectado.

2. Cuando el responsable del tratamiento contrate la prestación de un servicio que comporte un tratamiento de datos personales sometido a lo dispuesto en este capítulo deberá velar por que el encargado del tratamiento reúna las garantías para el cumplimiento de lo dispuesto en este Reglamento.

3. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato al que se refiere el apartado 2 del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

No obstante, el encargado del tratamiento no incurrirá en responsabilidad cuando, previa indicación expresa del responsable, comunique los datos a un tercero designado por aquél, al que hubiera encomendado la prestación de un servicio conforme a lo previsto en el presente capítulo.

Artículo 21. *Posibilidad de subcontratación de los servicios.*

1. El encargado del tratamiento no podrá subcontratar con un tercero la realización de ningún tratamiento que le hubiera encomendado el responsable del tratamiento, salvo que hubiera obtenido de éste autorización para ello. En este caso, la contratación se efectuará siempre en nombre y por cuenta del responsable del tratamiento.

2. No obstante lo dispuesto en el apartado anterior, será posible la subcontratación sin necesidad de autorización siempre y cuando se cumplan los siguientes requisitos:

a) Que se especifiquen en el contrato los servicios que puedan ser objeto de subcontratación y, si ello fuera posible, la empresa con la que se vaya a subcontratar.

Cuando no se identificase en el contrato la empresa con la que se vaya a subcontratar, será preciso que el encargado del tratamiento comunique al responsable los datos que la identifiquen antes de proceder a la subcontratación.

b) Que el tratamiento de datos de carácter personal por parte del subcontratista se ajuste a las instrucciones del responsable del fichero.

c) Que el encargado del tratamiento y la empresa subcontratista formalicen el contrato, en los términos previstos en el artículo anterior.

En este caso, el subcontratista será considerado encargado del tratamiento, siéndole de aplicación lo previsto en el artículo 20.3 de este reglamento.

3. Si durante la prestación del servicio resultase necesario subcontratar una parte del mismo y dicha circunstancia no hubiera sido prevista en el contrato, deberán someterse al responsable del tratamiento los extremos señalados en el apartado anterior.

Artículo 22. *Conservación de los datos por el encargado del tratamiento.*

1. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento o al encargado que éste hubiese designado, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

No procederá la destrucción de los datos cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos garantizando el responsable del fichero dicha conservación.

2. El encargado del tratamiento conservará, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.

TÍTULO III

Derechos de acceso, rectificación, cancelación y oposición

CAPÍTULO I

Disposiciones generales

Artículo 23. *Carácter personalísimo.*

1. Los derechos de acceso, rectificación, cancelación y oposición son personalísimos y serán ejercidos por el afectado.

2. Tales derechos se ejercitarán:

a) Por el afectado, acreditando su identidad, del modo previsto en el artículo siguiente.

b) Cuando el afectado se encuentre en situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal de estos derechos, podrán ejercitarse por su representante legal, en cuyo caso será necesario que acredite tal condición.

c) Los derechos también podrán ejercitarse a través de representante voluntario, expresamente designado para el ejercicio del derecho. En ese caso, deberá constar claramente acreditada la identidad del representado, mediante la aportación de copia de su Documento Nacional de Identidad o documento equivalente, y la representación conferida por aquél.

Cuando el responsable del fichero sea un órgano de las Administraciones públicas o de la Administración de Justicia, podrá acreditarse la representación por cualquier medio válido en derecho que deje constancia fidedigna, o mediante declaración en comparecencia personal del interesado.

3. Los derechos serán denegados cuando la solicitud sea formulada por persona distinta del afectado y no se acreditase que la misma actúa en representación de aquél.

Artículo 24. *Condiciones generales para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.*

1. Los derechos de acceso, rectificación, cancelación y oposición son derechos independientes, de tal forma que no puede entenderse que el ejercicio de ninguno de ellos sea requisito previo para el ejercicio de otro.

2. Deberá concederse al interesado un medio sencillo y gratuito para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

3. El ejercicio por el afectado de sus derechos de acceso, rectificación, cancelación y oposición será gratuito y en ningún caso podrá suponer un ingreso adicional para el responsable del tratamiento ante el que se ejercitan.

No se considerarán conformes a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente Reglamento los supuestos en que el responsable del tratamiento establezca como medio para que el interesado pueda ejercitar sus derechos el envío de cartas certificadas o semejantes, la utilización de servicios de telecomunicaciones que implique una tarificación adicional al afectado o cualesquiera otros medios que impliquen un coste excesivo para el interesado.

4. Cuando el responsable del fichero o tratamiento disponga de servicios de cualquier índole para la atención a su público o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados al mismo, podrá concederse la posibilidad al afectado de ejercer sus derechos de acceso, rectificación, cancelación y oposición a través de dichos servicios. En tal caso, la identidad del interesado se considerará acreditada por los medios establecidos para la identificación de los clientes del responsable en la prestación de sus servicios o contratación de sus productos.

5. El responsable del fichero o tratamiento deberá atender la solicitud de acceso, rectificación, cancelación u oposición ejercida por el afectado aún cuando el mismo no hubiese utilizado el procedimiento establecido específicamente al efecto por aquél, siempre que el interesado haya utilizado un medio que permita acreditar el envío y la recepción de la solicitud, y que ésta contenga los elementos referidos en el párrafo 1 del artículo siguiente.

Artículo 25. *Procedimiento.*

1. Salvo en el supuesto referido en el párrafo 4 del artículo anterior, el ejercicio de los derechos deberá llevarse a cabo mediante comunicación dirigida al responsable del fichero, que contendrá:

a) Nombre y apellidos del interesado; fotocopia de su documento nacional de identidad, o de su pasaporte u otro documento válido que lo identifique y, en su caso, de la persona que lo represente, o instrumentos electrónicos equivalentes; así como el documento o instrumento electrónico acreditativo de tal representación. La utilización de firma electrónica identificativa del afectado eximirá de la presentación de las fotocopias del DNI o documento equivalente.

El párrafo anterior se entenderá sin perjuicio de la normativa específica aplicable a la comprobación de datos de identidad por las Administraciones Públicas en los procedimientos administrativos.

b) Petición en que se concreta la solicitud.

c) Dirección a efectos de notificaciones, fecha y firma del solicitante.

d) Documentos acreditativos de la petición que formula, en su caso.

2. El responsable del tratamiento deberá contestar la solicitud que se le dirija en todo caso, con independencia de que figuren o no datos personales del afectado en sus ficheros.

3. En el caso de que la solicitud no reúna los requisitos especificados en el apartado primero, el responsable del fichero deberá solicitar la subsanación de los mismos.

4. La respuesta deberá ser conforme con los requisitos previstos para cada caso en el presente título.

5. Corresponderá al responsable del tratamiento la prueba del cumplimiento del deber de respuesta al que se refiere el apartado 2, debiendo conservar la acreditación del cumplimiento del mencionado deber.

6. El responsable del fichero deberá adoptar las medidas oportunas para garantizar que las personas de su organización que tienen acceso a datos de carácter personal puedan informar del procedimiento a seguir por el afectado para el ejercicio de sus derechos.

7. El ejercicio de los derechos de acceso, rectificación, cancelación y oposición podrá modularse por razones de seguridad pública en los casos y con el alcance previsto en las Leyes.

8. Cuando las leyes aplicables a determinados ficheros concretos establezcan un procedimiento especial para la rectificación o cancelación de los datos contenidos en los mismos, se estará a lo dispuesto en aquéllas.

Artículo 26. *Ejercicio de los derechos ante un encargado del tratamiento.*

Cuando los afectados ejercitasen sus derechos ante un encargado del tratamiento y solicitasen el ejercicio de su derecho ante el mismo, el encargado deberá dar traslado de la solicitud al responsable, a fin de que por el mismo se resuelva, a menos que en la relación existente con el responsable del tratamiento se prevea precisamente que el encargado atenderá, por cuenta del responsable, las solicitudes de ejercicio por los afectados de sus derechos de acceso, rectificación, cancelación u oposición.

CAPÍTULO II

Derecho de acceso

Artículo 27. *Derecho de acceso.*

1. El derecho de acceso es el derecho del afectado a obtener información sobre si sus propios datos de carácter personal están siendo objeto de tratamiento, la finalidad del tratamiento que, en su caso, se esté realizando, así como la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de los mismos.

2. En virtud del derecho de acceso el afectado podrá obtener del responsable del tratamiento información relativa a datos concretos, a datos incluidos en un determinado fichero, o a la totalidad de sus datos sometidos a tratamiento.

No obstante, cuando razones de especial complejidad lo justifiquen, el responsable del fichero podrá solicitar del afectado la especificación de los ficheros respecto de los cuales quiera ejercitar el derecho de acceso, a cuyo efecto deberá facilitarle una relación de todos ellos.

3. El derecho de acceso es independiente del que otorgan a los afectados las leyes especiales y en particular la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Artículo 28. *Ejercicio del derecho de acceso.*

1. Al ejercitar el derecho de acceso, el afectado podrá optar por recibir la información a través de uno o varios de los siguientes sistemas de consulta del fichero:

a) Visualización en pantalla.
b) Escrito, copia o fotocopia remitida por correo, certificado o no.
c) Telecopia.
d) Correo electrónico u otros sistemas de comunicaciones electrónicas.
e) Cualquier otro sistema que sea adecuado a la configuración o implantación material del fichero o a la naturaleza del tratamiento, ofrecido por el responsable.

2. Los sistemas de consulta del fichero previstos en el apartado anterior podrán restringirse en función de la configuración o implantación material del fichero o de la naturaleza del tratamiento, siempre que el que se ofrezca al afectado sea gratuito y asegure la comunicación escrita si éste así lo exige.
3. El responsable del fichero deberá cumplir al facilitar el acceso lo establecido en el Título VIII de este Reglamento.

Si tal responsable ofreciera un determinado sistema para hacer efectivo el derecho de acceso y el afectado lo rechazase, aquél no responderá por los posibles riesgos que para la seguridad de la información pudieran derivarse de la elección.
Del mismo modo, si el responsable ofreciera un procedimiento para hacer efectivo el derecho de acceso y el afectado exigiese que el mismo se materializase a través de un procedimiento que implique un coste desproporcionado, surtiendo el mismo efecto y garantizando la misma seguridad el procedimiento ofrecido por el responsable, serán de cuenta del afectado los gastos derivados de su elección.

Artículo 29. *Otorgamiento del acceso.*

1. El responsable del fichero resolverá sobre la solicitud de acceso en el plazo máximo de un mes a contar desde la recepción de la solicitud. Transcurrido el plazo sin que de forma expresa se responda a la petición de acceso, el interesado podrá interponer la reclamación prevista en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre.
En el caso de que no disponga de datos de carácter personal de los afectados deberá igualmente comunicárselo en el mismo plazo.
2. Si la solicitud fuera estimada y el responsable no acompañase a su comunicación la información a la que se refiere el artículo 27.1, el acceso se hará efectivo durante los diez días siguientes a dicha comunicación.
3. La información que se proporcione, cualquiera que sea el soporte en que fuere facilitada, se dará en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.
Dicha información comprenderá todos los datos de base del afectado, los resultantes de cualquier elaboración o proceso informático, así como la información disponible sobre el origen de los datos, los cesionarios de los mismos y la especificación de los concretos usos y finalidades para los que se almacenaron los datos.

Artículo 30. *Denegación del acceso.*

1. El responsable del fichero o tratamiento podrá denegar el acceso a los datos de carácter personal cuando el derecho ya se haya ejercitado en los doce meses anteriores a la solicitud, salvo que se acredite un interés legítimo al efecto.
2. Podrá también denegarse el acceso en los supuestos en que así lo prevea una Ley o una norma de derecho comunitario de aplicación directa o cuando éstas impidan al responsable del tratamiento revelar a los afectados el tratamiento de los datos a los que se refiera el acceso.
3. En todo caso, el responsable del fichero informará al afectado de su derecho a recabar la tutela de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas, conforme a lo dispuesto en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre.

CAPÍTULO III

Derechos de rectificación y cancelación

Artículo 31. *Derechos de rectificación y cancelación.*

1. El derecho de rectificación es el derecho del afectado a que se modifiquen los datos que resulten ser inexactos o incompletos.

2. El ejercicio del derecho de cancelación dará lugar a que se supriman los datos que resulten ser inadecuados o excesivos, sin perjuicio del deber de bloqueo conforme a este reglamento.

En los supuestos en que el interesado invoque el ejercicio del derecho de cancelación para revocar el consentimiento previamente prestado, se estará a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre y en el presente reglamento.

Artículo 32. *Ejercicio de los derechos de rectificación y cancelación.*

1. La solicitud de rectificación deberá indicar a qué datos se refiere y la corrección que haya de realizarse y deberá ir acompañada de la documentación justificativa de lo solicitado.

En la solicitud de cancelación, el interesado deberá indicar a qué datos se refiere, aportando al efecto la documentación que lo justifique, en su caso.

2. El responsable del fichero resolverá sobre la solicitud de rectificación o cancelación en el plazo máximo de diez días a contar desde la recepción de la solicitud. Transcurrido el plazo sin que de forma expresa se responda a la petición, el interesado podrá interponer la reclamación prevista en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre.

En el caso de que no disponga de datos de carácter personal del afectado deberá igualmente comunicárselo en el mismo plazo.

3. Si los datos rectificados o cancelados hubieran sido cedidos previamente, el responsable del fichero deberá comunicar la rectificación o cancelación efectuada al cesionario, en idéntico plazo, para que éste, también en el plazo de diez días contados desde la recepción de dicha comunicación, proceda, asimismo, a rectificar o cancelar los datos.

La rectificación o cancelación efectuada por el cesionario no requerirá comunicación alguna al interesado, sin perjuicio del ejercicio de los derechos por parte de los interesados reconocidos en la Ley Orgánica 15/1999, de 13 de diciembre.

Artículo 33. *Denegación de los derechos de rectificación y cancelación.*

1. La cancelación no procederá cuando los datos de carácter personal deban ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado que justificaron el tratamiento de los datos.

2. Podrá también denegarse los derechos de rectificación o cancelación en los supuestos en que así lo prevea una ley o una norma de derecho comunitario de aplicación directa o cuando éstas impidan al responsable del tratamiento revelar a los afectados el tratamiento de los datos a los que se refiera el acceso.

3. En todo caso, el responsable del fichero informará al afectado de su derecho a recabar la tutela de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las Comunidades Autónomas, conforme a lo dispuesto en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre.

CAPÍTULO IV

Derecho de oposición

Artículo 34. *Derecho de oposición.*

El derecho de oposición es el derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo en los siguientes supuestos:

a) Cuando no sea necesario su consentimiento para el tratamiento, como consecuencia de la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, siempre que una Ley no disponga lo contrario.

b) Cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial, en los términos previstos en el artículo 51 de este reglamento, cualquiera que sea la empresa responsable de su creación.

c) Cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal, en los términos previstos en el artículo 36 de este reglamento.

Artículo 35. *Ejercicio del derecho de oposición.*

1. El derecho de oposición se ejercitará mediante solicitud dirigida al responsable del tratamiento.

Cuando la oposición se realice con base en la letra a) del artículo anterior, en la solicitud deberán hacerse constar los motivos fundados y legítimos, relativos a una concreta situación personal del afectado, que justifican el ejercicio de este derecho.

2. El responsable del fichero resolverá sobre la solicitud de oposición en el plazo máximo de diez días a contar desde la recepción de la solicitud. Transcurrido el plazo sin que de forma expresa se responda a la petición, el interesado podrá interponer la reclamación prevista en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre.

En el caso de que no disponga de datos de carácter personal de los afectados deberá igualmente comunicárselo en el mismo plazo.

3. El responsable del fichero o tratamiento deberá excluir del tratamiento los datos relativos al afectado que ejercite su derecho de oposición o denegar motivadamente la solicitud del interesado en el plazo previsto en el apartado 2 de este artículo.

Artículo 36. *Derecho de oposición a las decisiones basadas únicamente en un tratamiento automatizado de datos.*

1. Los interesados tienen derecho a no verse sometidos a una decisión con efectos jurídicos sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, tales como su rendimiento laboral, crédito, fiabilidad o conducta.

2. No obstante, los afectados podrán verse sometidos a una de las decisiones contempladas en el apartado 1 cuando dicha decisión:

a) Se haya adoptado en el marco de la celebración o ejecución de un contrato a petición del interesado, siempre que se le otorgue la posibilidad de alegar lo que estimara pertinente, a fin de defender su derecho o interés. En todo caso, el responsable del fichero deberá informar previamente al afectado, de forma clara y precisa, de que se adoptarán decisiones con las características señaladas en el apartado 1 y cancelará los datos en caso de que no llegue a celebrarse finalmente el contrato.

b) Esté autorizada por una norma con rango de Ley que establezca medidas que garanticen el interés legítimo del interesado.

TÍTULO IV

Disposiciones aplicables a determinados ficheros de titularidad privada

CAPÍTULO I

Ficheros de información sobre solvencia patrimonial y crédito

Sección 1.ª Disposiciones generales

Artículo 37. *Régimen aplicable.*

1. El tratamiento de datos de carácter personal sobre solvencia patrimonial y crédito, previsto en el apartado 1 del artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre, se

someterá a lo establecido, con carácter general, en dicha ley orgánica y en el presente reglamento.

2. El ejercicio de los derechos de acceso, rectificación, cancelación y oposición en el caso de los ficheros a que se refiere el apartado anterior, se rige por lo dispuesto en los capítulos I a IV del título III del presente reglamento, con los siguientes criterios:

a) Cuando la petición de ejercicio de los derechos se dirigiera al responsable del fichero, éste estará obligado a satisfacer, en cualquier caso, dichos derechos.

b) Si la petición se dirigiera a las personas y entidades a las que se presta el servicio, éstas únicamente deberán comunicar al afectado aquellos datos relativos al mismo que les hayan sido comunicados y a facilitar la identidad del responsable para que, en su caso, puedan ejercitar sus derechos ante el mismo.

3. De conformidad con el apartado 2 del artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre, también podrán tratarse los datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés.

Estos datos deberán conservarse en ficheros creados con la exclusiva finalidad de facilitar información crediticia del afectado y su tratamiento se regirá por lo dispuesto en el presente reglamento y, en particular, por las previsiones contenidas en la sección segunda de este capítulo.

Sección 2.ª Tratamiento de datos relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés

Artículo 38. *Requisitos para la inclusión de los datos.*

1. Sólo será posible la inclusión en estos ficheros de datos de carácter personal que sean determinantes para enjuiciar la solvencia económica del afectado, siempre que concurran los siguientes requisitos:

a) Existencia previa de una deuda cierta, vencida, exigible, que haya resultado impagada **y respecto de la cual no se haya entablado reclamación judicial, arbitral o administrativa, o tratándose de servicios financieros, no se haya planteado una reclamación en los términos previstos en el Reglamento de los Comisionados para la defensa del cliente de servicios financieros, aprobado por Real Decreto 303/2004, de 20 de febrero.**

> Téngase en cuenta que se anula el inciso destacado de la letra a) del apartado 1 por Sentencias del TS de 15 de julio de 2010. Ref. BOE-A-2010-16299 y Ref. BOE-A-2010-16301

b) Que no hayan transcurrido seis años desde la fecha en que hubo de procederse al pago de la deuda o del vencimiento de la obligación o del plazo concreto si aquélla fuera de vencimiento periódico.

c) Requerimiento previo de pago a quien corresponda el cumplimiento de la obligación.

2. **(Anulado)**

3. El acreedor o quien actúe por su cuenta o interés estará obligado a conservar a disposición del responsable del fichero común y de la Agencia Española de Protección de Datos documentación suficiente que acredite el cumplimiento de los requisitos establecidos en este artículo y del requerimiento previo al que se refiere el artículo siguiente.

Artículo 39. *Información previa a la inclusión.*

El acreedor deberá informar al deudor, en el momento en que se celebre el contrato y, en todo caso, al tiempo de efectuar el requerimiento al que se refiere la letra c) del apartado 1 del artículo anterior, que en caso de no producirse el pago en el término previsto para ello y cumplirse los requisitos previstos en el citado artículo, los datos relativos al impago podrán

ser comunicados a ficheros relativos al cumplimiento o incumplimiento de obligaciones dinerarias.

Artículo 40. *Notificación de inclusión.*

1. El responsable del fichero común deberá notificar a los interesados respecto de los que hayan registrado datos de carácter personal, en el plazo de treinta días desde dicho registro, una referencia de los que hubiesen sido incluidos, informándole asimismo de la posibilidad de ejercitar sus derechos de acceso, rectificación, cancelación y oposición, en los términos establecidos por la Ley Orgánica 15/1999, de 13 de diciembre.

2. Se efectuará una notificación por cada deuda concreta y determinada con independencia de que ésta se tenga con el mismo o con distintos acreedores.

3. La notificación deberá efectuarse a través de un medio fiable, auditable e independiente de la entidad notificante, que la permita acreditar la efectiva realización de los envíos.

4. En todo caso, será necesario que el responsable del fichero pueda conocer si la notificación ha sido objeto de devolución por cualquier causa, en cuyo caso no podrá proceder al tratamiento de los datos referidos a ese interesado.

No se entenderán suficientes para que no se pueda proceder al tratamiento de los datos referidos a un interesado las devoluciones en las que el destinatario haya rehusado recibir el envío.

5. Si la notificación de inclusión fuera devuelta, el responsable del fichero común comprobará con la entidad acreedora que la dirección utilizada para efectuar esta notificación se corresponde con la contractualmente pactada con el cliente a efectos de comunicaciones y no procederá al tratamiento de los datos si la mencionada entidad no confirma la exactitud de este dato.

Artículo 41. *Conservación de los datos.*

1. Sólo podrán ser objeto de tratamiento los datos que respondan con veracidad a la situación de la deuda en cada momento concreto.

El pago o cumplimiento de la deuda determinará la cancelación inmediata de todo dato relativo a la misma.

2. En los restantes supuestos, los datos deberán ser cancelados cuando se hubieran cumplido seis años contados a partir del vencimiento de la obligación o del plazo concreto si aquélla fuera de vencimiento periódico.

Artículo 42. *Acceso a la información contenida en el fichero.*

1. Los datos contenidos en el fichero común sólo podrán ser consultados por terceros cuando precisen enjuiciar la solvencia económica del afectado. En particular, se considerará que concurre dicha circunstancia en los siguientes supuestos:

a) Que el afectado mantenga con el tercero algún tipo de relación contractual que aún no se encuentre vencida.

b) Que el afectado pretenda celebrar con el tercero un contrato que implique el pago aplazado del precio.

c) Que el afectado pretenda contratar con el tercero la prestación de un servicio de facturación periódica.

2. Los terceros deberán informar por escrito a las personas en las que concurran los supuestos contemplados en las letras b) y c) precedentes de su derecho a consultar el fichero.

En los supuestos de contratación telefónica de los productos o servicios a los que se refiere el párrafo anterior, la información podrá realizarse de forma no escrita, correspondiendo al tercero la prueba del cumplimiento del deber de informar.

Artículo 43. *Responsabilidad.*

1. El acreedor o quien actúe por su cuenta o interés deberá asegurarse que concurren todos los requisitos exigidos en los artículos 38 y 39 en el momento de notificar los datos adversos al responsable del fichero común.

2. El acreedor o quien actúe por su cuenta o interés será responsable de la inexistencia o inexactitud de los datos que hubiera facilitado para su inclusión en el fichero, en los términos previstos en la Ley Orgánica 15/1999, de 13 de diciembre.

Artículo 44. *Ejercicio de los derechos de acceso, rectificación, cancelación y oposición.*

1. El ejercicio de los derechos de acceso, rectificación, cancelación y oposición se rige por lo dispuesto en los capítulos I a IV del título III de este reglamento, sin perjuicio de lo señalado en el presente artículo.

2. Cuando el interesado ejercite su derecho de acceso en relación con la inclusión de sus datos en un fichero regulado por el artículo 29.2 de la Ley Orgánica 15/1999, de 13 de diciembre, se tendrán en cuenta las siguientes reglas:

1.ª Si la solicitud se dirigiera al titular del fichero común, éste deberá comunicar al afectado todos los datos relativos al mismo que obren en el fichero.

En este caso, el titular del fichero común deberá, además de dar cumplimiento a lo establecido en el presente reglamento, facilitar las evaluaciones y apreciaciones que sobre el afectado se hayan comunicado en los últimos seis meses y el nombre y dirección de los cesionarios.

2.ª Si la solicitud se dirigiera a cualquier otra entidad participante en el sistema, deberá comunicar al afectado todos los datos relativos al mismo a los que ella pueda acceder, así como la identidad y dirección del titular del fichero común para que pueda completar el ejercicio de su derecho de acceso.

3. Cuando el interesado ejercite sus derechos de rectificación o cancelación en relación con la inclusión de sus datos en un fichero regulado por el artículo 29.2 de la Ley Orgánica 15/1999, de 13 de diciembre, se tendrán en cuenta las siguientes reglas:

1.ª Si la solicitud se dirige al titular del fichero común, éste tomará las medidas oportunas para trasladar dicha solicitud a la entidad que haya facilitado los datos, para que ésta la resuelva. En el caso de que el responsable del fichero común no haya recibido contestación por parte de la entidad en el plazo de siete días, procederá a la rectificación o cancelación cautelar de los mismos.

2.ª Si la solicitud se dirige a quien haya facilitado los datos al fichero común procederá a la rectificación o cancelación de los mismos en sus ficheros y a notificarlo al titular del fichero común en el plazo de diez días, dando asimismo respuesta al interesado en los términos previstos en el artículo 33 de este reglamento.

3.ª Si la solicitud se dirige a otra entidad participante en el sistema, que no hubiera facilitado al fichero común los datos, dicha entidad informará al afectado sobre este hecho en el plazo máximo de diez días, proporcionándole, además, la identidad y dirección del titular del fichero común para, que en su caso, puedan ejercitar sus derechos ante el mismo.

CAPÍTULO II

Tratamientos para actividades de publicidad y prospección comercial

Artículo 45. *Datos susceptibles de tratamiento e información al interesado.*

1. Quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades análogas, así como quienes realicen estas actividades con el fin de comercializar sus propios productos o servicios o los de terceros, sólo podrán utilizar nombres y direcciones u otros datos de carácter personal cuando los mismos se encuentren en uno de los siguientes casos:

a) Figuren en alguna de las fuentes accesibles al público a las que se refiere la letra j) del artículo 3 de la Ley Orgánica 15/1999, de 13 de diciembre y el artículo 7 de este

reglamento y el interesado no haya manifestado su negativa u oposición a que sus datos sean objeto de tratamiento para las actividades descritas en este apartado.

b) Hayan sido facilitados por los propios interesados u obtenidos con su consentimiento para finalidades determinadas, explícitas y legítimas relacionadas con la actividad de publicidad o prospección comercial, habiéndose informado a los interesados sobre los sectores específicos y concretos de actividad respecto de los que podrá recibir información o publicidad.

2. Cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, deberá informarse al interesado en cada comunicación que se le dirija del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten, con indicación de ante quién podrán ejercitarse.

A tal efecto, el interesado deberá ser informado de que sus datos han sido obtenidos de fuentes accesibles al público y de la entidad de la que hubieran sido obtenidos.

Artículo 46. *Tratamiento de datos en campañas publicitarias.*

1. Para que una entidad pueda realizar por sí misma una actividad publicitaria de sus productos o servicios entre sus clientes será preciso que el tratamiento se ampare en alguno de los supuestos contemplados en el artículo 6 de la Ley Orgánica 15/1999, de 13 de diciembre.

2. En caso de que una entidad contrate o encomiende a terceros la realización de una determinada campaña publicitaria de sus productos o servicios, encomendándole el tratamiento de determinados datos, se aplicarán las siguientes normas:

a) Cuando los parámetros identificativos de los destinatarios de la campaña sean fijados por la entidad que contrate la campaña, ésta será responsable del tratamiento de los datos.

b) Cuando los parámetros fueran determinados únicamente por la entidad o entidades contratadas, dichas entidades serán las responsable del tratamiento.

c) Cuando en la determinación de los parámetros intervengan ambas entidades, serán ambas responsables del tratamiento.

3. En el supuesto contemplado en el apartado anterior, la entidad que encargue la realización de la campaña publicitaria deberá adoptar las medidas necesarias para asegurarse de que la entidad contratada ha recabado los datos cumpliendo las exigencias establecidas en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente reglamento.

4. A los efectos previstos en este artículo, se consideran parámetros identificativos de los destinatarios las variables utilizadas para identificar el público objetivo o destinatario de una campaña o promoción comercial de productos o servicios que permitan acotar los destinatarios individuales de la misma.

Artículo 47. *Depuración de datos personales.*

Cuando dos o más responsables por sí mismos o mediante encargo a terceros pretendieran constatar sin consentimiento de los afectados, con fines de promoción o comercialización de sus productos o servicios y mediante un tratamiento cruzado de sus ficheros quiénes ostentan la condición de clientes de una u otra o de varios de ellos, el tratamiento así realizado constituirá una cesión o comunicación de datos.

Artículo 48. *Ficheros de exclusión del envío de comunicaciones comerciales.*

Los responsables a los que el afectado haya manifestado su negativa a recibir publicidad podrán conservar los mínimos datos imprescindibles para identificarlo y adoptar las medidas necesarias que eviten el envío de publicidad.

Artículo 49. *Ficheros comunes de exclusión del envío de comunicaciones comerciales.*

1. Será posible la creación de ficheros comunes, de carácter general o sectorial, en los que sean objeto de tratamiento los datos de carácter personal que resulten necesarios para

evitar el envío de comunicaciones comerciales a los interesados que manifiesten su negativa u oposición a recibir publicidad.

A tal efecto, los citados ficheros podrán contener los mínimos datos imprescindibles para identificar al afectado.

2. Cuando el afectado manifieste ante un concreto responsable su negativa u oposición a que sus datos sean tratados con fines de publicidad o prospección comercial, aquél deberá ser informado de la existencia de los ficheros comunes de exclusión generales o sectoriales, así como de la identidad de su responsable, su domicilio y la finalidad del tratamiento.

El afectado podrá solicitar su exclusión respecto de un fichero o tratamiento concreto o su inclusión en ficheros comunes de excluidos de carácter general o sectorial.

3. La entidad responsable del fichero común podrá tratar los datos de los interesados que hubieran manifestado su negativa u oposición al tratamiento de sus datos con fines de publicidad o prospección comercial, cumpliendo las restantes obligaciones establecidas en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente Reglamento.

4. Quienes pretendan efectuar un tratamiento relacionado con actividades de publicidad o prospección comercial deberán previamente consultar los ficheros comunes que pudieran afectar a su actuación, a fin de evitar que sean objeto de tratamiento los datos de los afectados que hubieran manifestado su oposición o negativa a ese tratamiento.

Artículo 50. *Derechos de acceso, rectificación y cancelación.*

1. El ejercicio de los derechos de acceso, rectificación y cancelación en relación con los tratamientos vinculados a actividades de publicidad y prospección comercial se someterá a lo previsto en los capítulos I a IV del título III de este reglamento.

2. Si el derecho se ejercitase ante una entidad que hubiese encargado a un tercero la realización de una campaña publicitaria, aquélla estará obligada, en el plazo de diez días, desde la recepción de la comunicación de la solicitud de ejercicio de derechos del afectado, a comunicar la solicitud al responsable del fichero a fin de que el mismo otorgue al afectado su derecho en el plazo de diez días desde la recepción de la comunicación, dando cuenta de ello al afectado.

Lo dispuesto en el párrafo anterior se entenderá sin perjuicio del deber impuesto a la entidad mencionada en el apartado anterior, en todo caso, por el párrafo segundo del artículo 5.5 de la Ley Orgánica 15/1999, de 13 de diciembre.

Artículo 51. *Derecho de oposición.*

1. Los interesados tendrán derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que les conciernan, en cuyo caso serán dados de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud.

La oposición a la que se refiere el párrafo anterior deberá entenderse sin perjuicio del derecho del interesado a revocar cuando lo estimase oportuno el consentimiento que hubiera otorgado, en su caso, para el tratamiento de los datos.

2. A tal efecto, deberá concederse al interesado un medio sencillo y gratuito para oponerse al tratamiento. En particular, se considerará cumplido lo dispuesto en este precepto cuando los derechos puedan ejercitarse mediante la llamada a un número telefónico gratuito o la remisión de un correo electrónico.

3. Cuando el responsable del fichero o tratamiento disponga de servicios de cualquier índole para la atención a sus clientes o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados al mismo, deberá concederse la posibilidad al afectado de ejercer su oposición a través de dichos servicios.

No se considerarán conformes a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, los supuestos en que el responsable del tratamiento establezca como medio para que el interesado pueda ejercitar su oposición el envío de cartas certificadas o envíos semejantes, la utilización de servicios de telecomunicaciones que implique una tarificación adicional al afectado o cualesquiera otros medios que impliquen un coste excesivo para el interesado.

En todo caso, el ejercicio por el afectado de sus derechos no podrá suponer un ingreso adicional para el responsable del tratamiento ante el que se ejercitan.

4. Si el derecho de oposición se ejercitase ante una entidad que hubiera encomendado a un tercero la realización de una campaña publicitaria, aquélla estará obligada, en el plazo de diez días, desde la recepción de la comunicación de la solicitud de ejercicio de derechos del afectado, a comunicar la solicitud al responsable del fichero a fin de que el mismo atienda el derecho del afectado en el plazo de diez días desde la recepción de la comunicación, dando cuenta de ello al afectado.

Lo dispuesto en el párrafo anterior se entenderá sin perjuicio del deber impuesto a la entidad mencionada en el apartado anterior, en todo caso, por el párrafo segundo del artículo 5.5 de la Ley Orgánica 15/1999, de 13 de diciembre.

TÍTULO V

Obligaciones previas al tratamiento de los datos

CAPÍTULO I

Creación, modificación o supresión de ficheros de titularidad pública

Artículo 52. *Disposición o Acuerdo de creación, modificación o supresión del fichero.*

1. La creación, modificación o supresión de los ficheros de titularidad pública sólo podrá hacerse por medio de disposición general o acuerdo publicados en el «Boletín Oficial del Estado» o diario oficial correspondiente.

2. En todo caso, la disposición o acuerdo deberá dictarse y publicarse con carácter previo a la creación, modificación o supresión del fichero.

Artículo 53. *Forma de la disposición o acuerdo.*

1. Cuando la disposición se refiera a los órganos de la Administración General del Estado o a las entidades u organismos vinculados o dependientes de la misma, deberá revestir la forma de orden ministerial o resolución del titular de la entidad u organismo correspondiente.

2. En el caso de los órganos constitucionales del Estado, se estará a lo que establezcan sus normas reguladoras.

3. En relación con los ficheros de los que sean responsables las comunidades autónomas, entidades locales y las entidades u organismos vinculados o dependientes de las mismas, las universidades públicas, así como los órganos de las comunidades autónomas con funciones análogas a los órganos constitucionales del Estado, se estará a su legislación específica.

4. La creación, modificación o supresión de los ficheros de los que sean responsables las corporaciones de derecho público y que se encuentren relacionados con el ejercicio por aquéllas de potestades de derecho público deberá efectuarse a través de acuerdo de sus órganos de gobierno, en los términos que establezcan sus respectivos Estatutos, debiendo ser igualmente objeto de publicación en el «Boletín Oficial del Estado» o diario oficial correspondiente.

Artículo 54. *Contenido de la disposición o acuerdo.*

1. La disposición o acuerdo de creación del fichero deberá contener los siguientes extremos:

a) La identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos.

b) El origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia.

c) La estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las

restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización.

d) Las comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios.

e) Las transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos.

f) Los órganos responsables del fichero.

g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.

h) El nivel básico, medio o alto de seguridad que resulte exigible, de acuerdo con lo establecido en el título VIII del presente reglamento.

2. La disposición o acuerdo de modificación del fichero deberá indicar las modificaciones producidas en cualquiera de los extremos a los que se refiere el apartado anterior.

3. En las disposiciones o acuerdos que se dicten para la supresión de los ficheros se establecerá el destino que vaya a darse a los datos o, en su caso, las previsiones que se adopten para su destrucción.

CAPÍTULO II

Notificación e inscripción de los ficheros de titularidad pública o privada

Artículo 55. *Notificación de ficheros.*

1. Todo fichero de datos de carácter personal de titularidad pública será notificado a la Agencia Española de Protección de Datos por el órgano competente de la Administración responsable del fichero para su inscripción en el Registro General de Protección de Datos, en el plazo de treinta días desde la publicación de su norma o acuerdo de creación en el diario oficial correspondiente.

2. Los ficheros de datos de carácter personal de titularidad privada serán notificados a la Agencia Española de Protección de Datos por la persona o entidad privada que pretenda crearlos, con carácter previo a su creación. La notificación deberá indicar la identificación del responsable del fichero, la identificación del fichero, sus finalidades y los usos previstos, el sistema de tratamiento empleado en su organización, el colectivo de personas sobre el que se obtienen los datos, el procedimiento y procedencia de los datos, las categorías de datos, el servicio o unidad de acceso, la indicación del nivel de medidas de seguridad básico, medio o alto exigible, y en su caso, la identificación del encargado del tratamiento en donde se encuentre ubicado el fichero y los destinatarios de cesiones y transferencias internacionales de datos.

3. Cuando la obligación de notificar afecte a ficheros sujetos a la competencia de la autoridad de control de una comunidad autónoma que haya creado su propio registro de ficheros, la notificación se realizará a la autoridad autonómica competente, que dará traslado de la inscripción al Registro General de Protección de Datos.

El Registro General de Protección de Datos podrá solicitar de las autoridades de control de las comunidades autónomas el traslado al que se refiere el párrafo anterior, procediendo, en su defecto, a la inclusión de oficio del fichero en el Registro.

4. La notificación se realizará conforme al procedimiento establecido en la sección primera del capítulo IV del título IX del presente reglamento.

Artículo 56. *Tratamiento de datos en distintos soportes.*

1. La notificación de un fichero de datos de carácter personal es independiente del sistema de tratamiento empleado en su organización y del soporte o soportes empleados para el tratamiento de los datos.

2. Cuando los datos de carácter personal objeto de un tratamiento estén almacenados en diferentes soportes, automatizados y no automatizados o exista una copia en soporte no automatizado de un fichero automatizado sólo será precisa una sola notificación, referida a dicho fichero.

Artículo 57. *Ficheros en los que exista más de un responsable.*

Cuando se tenga previsto crear un fichero del que resulten responsables varias personas o entidades simultáneamente, cada una de ellas deberá notificar, a fin de proceder a su inscripción en el Registro General de Protección de Datos y, en su caso, en los Registros de Ficheros creados por las autoridades de control de las comunidades autónomas, la creación del correspondiente fichero.

Artículo 58. *Notificación de la modificación o supresión de ficheros.*

1. La inscripción del fichero deberá encontrarse actualizada en todo momento. Cualquier modificación que afecte al contenido de la inscripción de un fichero deberá ser previamente notificada a la Agencia Española de Protección de Datos o a las autoridades de control autonómicas competentes, a fin de proceder a su inscripción en el registro correspondiente, conforme a lo dispuesto en el artículo 55.

2. Cuando el responsable del fichero decida su supresión, deberá notificarla a efectos de que se proceda a la cancelación de la inscripción en el registro correspondiente.

3. Tratándose de ficheros de titularidad pública, cuando se pretenda la modificación que afecte a alguno de los requisitos previstos en el artículo 55 o la supresión del fichero deberá haberse adoptado, con carácter previo a la notificación la correspondiente norma o acuerdo en los términos previstos en el capítulo I de este título.

Artículo 59. *Modelos y soportes para la notificación.*

1. La Agencia Española de Protección de Datos publicará mediante la correspondiente Resolución del Director los modelos o formularios electrónicos de notificación de creación, modificación o supresión de ficheros, que permitan su presentación a través de medios telemáticos o en soporte papel, así como, previa consulta de las autoridades de protección de datos de las comunidades autónomas, los formatos para la comunicación telemática de ficheros públicos por las autoridades de control autonómicas, de conformidad con lo establecido en los artículos 55 y 58 del presente reglamento.

2. Los modelos o formularios electrónicos de notificación se podrán obtener gratuitamente en la página web de la Agencia Española de Protección de Datos.

3. El Director de la Agencia Española de Protección de Datos podrá establecer procedimientos simplificados de notificación en atención a las circunstancias que concurran en el tratamiento o el tipo de fichero al que se refiera la notificación.

Artículo 60. *Inscripción de los ficheros.*

1. El Director de la Agencia Española de Protección de Datos, a propuesta del Registro General de Protección de Datos, dictará resolución acordando, en su caso, la inscripción, una vez tramitado el procedimiento previsto en el capítulo IV del título IX.

2. La inscripción contendrá el código asignado por el Registro, la identificación del responsable del fichero, la identificación del fichero o tratamiento, la descripción de su finalidad y usos previstos, el sistema de tratamiento empleado en su organización, en su caso, el colectivo de personas sobre el que se obtienen los datos, el procedimiento y procedencia de los datos, las categorías de datos, el servicio o unidad de acceso, y la indicación del nivel de medidas de seguridad exigible conforme a lo dispuesto en el artículo 81.

Asimismo, se incluirán, en su caso, la identificación del encargado del tratamiento en donde se encuentre ubicado el fichero y los destinatarios de cesiones y transferencias internacionales.

En el caso de ficheros de titularidad pública también se hará constar la referencia de la disposición general por la que ha sido creado, y en su caso, modificado.

3. La inscripción de un fichero en el Registro General de Protección de Datos, no exime al responsable del cumplimiento del resto de las obligaciones previstas en la Ley Orgánica 15/1999, de 13 de diciembre, y demás disposiciones reglamentarias.

Artículo 61. *Cancelación de la inscripción.*

1. Cuando el responsable del tratamiento comunicase, en virtud de lo dispuesto en el artículo 58 de este reglamento, la supresión del fichero, el Director de la Agencia Española de Protección de Datos, previa la tramitación del procedimiento establecido en la sección primera del capítulo IV del título IX, dictará resolución acordando la cancelación de la inscripción correspondiente al fichero.

2. El Director de la Agencia Española de Protección de Datos podrá, en ejercicio de sus competencias, acordar de oficio la cancelación de la inscripción de un fichero cuando concurran circunstancias que acrediten la imposibilidad de su existencia, previa la tramitación del procedimiento establecido en la sección segunda del capítulo IV del título IX de este reglamento.

Artículo 62. *Rectificación de errores.*

El Registro General de Protección de Datos podrá rectificar en cualquier momento, de oficio o a instancia de los interesados, los errores materiales, de hecho o aritméticos que pudieran existir en las inscripciones, de conformidad con lo dispuesto en el artículo 105 de la Ley 30/1992, de 26 de noviembre.

Artículo 63. *Inscripción de oficio de ficheros de titularidad pública.*

1. En supuestos excepcionales con el fin de garantizar el derecho a la protección de datos de los afectados, y sin perjuicio de la obligación de notificación, se podrá proceder a la inscripción de oficio de un determinado fichero en el Registro General de Protección de Datos.

2. Para que lo dispuesto en el apartado anterior resulte de aplicación, será requisito indispensable que la correspondiente norma o acuerdo regulador de los ficheros que contengan datos de carácter personal haya sido publicado en el correspondiente diario oficial y cumpla los requisitos establecidos en la Ley Orgánica 15/1999, de 13 de diciembre, y el presente reglamento.

3. El Director de la Agencia Española de Protección de Datos podrá, a propuesta del Registro General de Protección de Datos, acordar la inscripción del fichero de titularidad pública en el Registro, notificándose dicho acuerdo al órgano responsable del fichero.

Cuando la inscripción se refiera a ficheros sujetos a la competencia de la autoridad de control de una comunidad autónoma que haya creado su propio registro de ficheros, se comunicará a la referida autoridad de control autonómica para que proceda, en su caso, a la inscripción de oficio.

Artículo 64. *Colaboración con las autoridades de control de las comunidades autónomas.*

El Director de la Agencia Española de Protección de Datos podrá celebrar con los directores de las autoridades de control de las comunidades autónomas los convenios de colaboración o acuerdos que estime pertinentes, a fin de garantizar la inscripción en el Registro General de Protección de Datos de los ficheros sometidos a la competencia de dichas autoridades autonómicas.

TÍTULO VI

Transferencias internacionales de datos

CAPÍTULO I

Disposiciones generales

Artículo 65. *Cumplimiento de las disposiciones de la Ley Orgánica 15/1999, de 13 de diciembre.*

La transferencia internacional de datos no excluye en ningún caso la aplicación de las disposiciones contenidas en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente reglamento.

Artículo 66. *Autorización y notificación.*

1. Para que la transferencia internacional de datos pueda considerarse conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente Reglamento será necesaria la autorización del Director de la Agencia Española de Protección de Datos, que se otorgará en caso de que el exportador aporte las garantías a las que se refiere el artículo 70 del presente reglamento.

La autorización se otorgará conforme al procedimiento establecido en la sección primera del capítulo V del título IX de este reglamento.

2. La autorización no será necesaria:

a) Cuando el Estado en el que se encontrase el importador ofrezca un nivel adecuado de protección conforme a lo previsto en el capítulo II de este título.

b) Cuando la transferencia se encuentre en uno de los supuestos contemplados en los apartados a) a j) del artículo 34 de la Ley Orgánica 15/1999, de 13 de diciembre.

3. En todo caso, la transferencia internacional de datos deberá ser notificada a fin de proceder a su inscripción en el Registro General de Protección de Datos, conforme al procedimiento establecido en la sección primera del capítulo IV del título IX del presente reglamento.

CAPÍTULO II

Transferencias a estados que proporcionen un nivel adecuado de protección

Artículo 67. *Nivel adecuado de protección acordado por la Agencia Española de Protección de Datos.*

1. No será precisa autorización del Director de la Agencia Española de Protección de Datos a una transferencia internacional de datos cuando las normas aplicables al Estado en que se encontrase el importador ofrezcan dicho nivel adecuado de protección a juicio del Director de la Agencia Española de Protección de Datos.

El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

Las resoluciones del Director de la Agencia Española de Protección de Datos por las que se acordase que un determinado país proporciona un nivel adecuado de protección de datos serán publicadas en el «Boletín Oficial del Estado».

2. El Director de la Agencia Española de Protección de Datos acordará la publicación de la relación de países cuyo nivel de protección haya sido considerado equiparable conforme a lo dispuesto en el apartado anterior.

Esta lista se publicará y mantendrá actualizada asimismo a través de medios informáticos o telemáticos.

Artículo 68. *Nivel adecuado de protección declarado por Decisión de la Comisión Europea.*

No será necesaria la autorización del Director de la Agencia Española de Protección de Datos para la realización de una transferencia internacional de datos que tuvieran por importador una persona o entidad, pública o privada, situada en el territorio de un Estado respecto del que se haya declarado por la Comisión Europea la existencia de un nivel adecuado de protección.

Artículo 69. *Suspensión temporal de las transferencias.*

1. En los supuestos previstos en los artículos precedentes, el Director de la Agencia Española de Protección de Datos, en uso de la potestad que le otorga el artículo 37.1 f) de la Ley Orgánica 15/1999, de 13 de diciembre, podrá acordar, previa audiencia del exportador, la suspensión temporal de la transferencia de datos hacia un importador ubicado en un tercer Estado del que se haya declarado la existencia de un nivel adecuado de protección, cuando concurra alguna de las circunstancias siguientes:

a) Que las autoridades de Protección de Datos del Estado importador o cualquier otra competente, en caso de no existir las primeras, resuelvan que el importador ha vulnerado las normas de protección de datos establecidas en su derecho interno.

b) Que existan indicios racionales de que se estén vulnerando las normas o, en su caso, los principios de protección de datos por la entidad importadora de la transferencia y que las autoridades competentes en el Estado en que se encuentre el importador no han adoptado o no van a adoptar en el futuro las medidas oportunas para resolver el caso en cuestión, habiendo sido advertidas de la situación por la Agencia Española de Protección de Datos. En este caso se podrá suspender la transferencia cuando su continuación pudiera generar un riesgo inminente de grave perjuicio a los afectados.

2. La suspensión se acordará previa la tramitación del procedimiento establecido en la sección segunda del capítulo V del título IX del presente reglamento.

En estos casos, la decisión del Director de la Agencia Española de Protección de Datos será notificada a la Comisión Europea.

CAPÍTULO III

Transferencias a Estados que no proporcionen un nivel adecuado de protección

Artículo 70. *Transferencias sujetas a autorización del Director de la Agencia Española de Protección de Datos.*

1. Cuando la transferencia tenga por destino un Estado respecto del que no se haya declarado por la Comisión Europea o no se haya considerado por el Director de la Agencia Española de Protección de Datos que existe un nivel adecuado de protección, será necesario recabar la autorización del Director de la Agencia Española de Protección de Datos.

La autorización de la transferencia se tramitará conforme al procedimiento establecido en la sección primera del capítulo V del título IX del presente reglamento.

2. La autorización podrá ser otorgada en caso de que el responsable del fichero o tratamiento aporte un contrato escrito, celebrado entre el exportador y el importador, en el que consten las necesarias garantías de respeto a la protección de la vida privada de los afectados y a sus derechos y libertades fundamentales y se garantice el ejercicio de sus respectivos derechos.

A tal efecto, se considerará que establecen las adecuadas garantías los contratos que se celebren de acuerdo con lo previsto en las Decisiones de la Comisión Europea 2001/497/CE, de 15 de Junio de 2001, 2002/16/CE, de 27 de diciembre de 2001, y 2004/915/CE, de 27 de

diciembre de 2004 o de lo que dispongan las Decisiones de la Comisión que den cumplimiento a lo establecido en el artículo 26.4 de la Directiva 95/46/CE.

3. En el supuesto contemplado en el apartado anterior, el Director de la Agencia Española de Protección de Datos podrá denegar o, en uso de la potestad que le otorga el artículo 37.1 f) de la Ley Orgánica 15/1999, de 13 de diciembre, suspender temporalmente, previa audiencia del exportador, la transferencia, cuando concurra alguna de las circunstancias siguientes:

a) Que la situación de protección de los derechos fundamentales y libertades públicas en el país de destino o su legislación impidan garantizar el íntegro cumplimiento del contrato y el ejercicio por los afectados de los derechos que el contrato garantiza.

b) Que la entidad destinataria haya incumplido previamente las garantías establecidas en cláusulas contractuales de este tipo.

c) Que existan indicios racionales de que las garantías ofrecidas por el contrato no están siendo o no serán respetadas por el importador.

d) Que existan indicios racionales de que los mecanismos de aplicación del contrato no son o no serán efectivos.

e) Que la transferencia, o su continuación, en caso de haberse iniciado, pudiera crear una situación de riesgo de daño efectivo a los afectados.

La suspensión se acordará previa la tramitación del procedimiento establecido en la sección segunda del capítulo V del título IX del presente reglamento.

Las resoluciones del Director de la Agencia Española de Protección de Datos por las que se deniegue o suspenda una transferencia internacional de datos en virtud de las causas a las que se refiere este apartado serán notificadas a la Comisión de las Comunidades Europeas cuando así sea exigible.

4. También podrá otorgarse la autorización para la transferencia internacional de datos en el seno de grupos multinacionales de empresas cuando hubiesen sido adoptados por los mismos normas o reglas internas en que consten las necesarias garantías de respeto a la protección de la vida privada y el derecho fundamental a la protección de datos de los afectados y se garantice asimismo el cumplimiento de los principios y el ejercicio de los derechos reconocidos en la Ley Orgánica 15/1999, de 13 de diciembre, y el presente reglamento.

En este caso, para que proceda la autorización del Director de la Agencia Española de Protección de Datos será preciso que las normas o reglas resulten vinculantes para las empresas del Grupo y exigibles conforme al ordenamiento jurídico español.

En todo caso, la autorización del Director de la Agencia Española de Protección de Datos implicará la exigibilidad de lo previsto en las normas o reglas internas tanto por la Agencia como por los afectados cuyos datos hubieran sido objeto de tratamiento.

TÍTULO VII

Códigos tipo

Artículo 71. *Objeto y naturaleza.*

1. Los códigos tipo a los que se refiere el artículo 32 de la Ley Orgánica 15/1999, de 13 de diciembre, tienen por objeto adecuar lo establecido en la citada Ley Orgánica y en el presente reglamento a las peculiaridades de los tratamientos efectuados por quienes se adhieren a los mismos.

A tal efecto, contendrán reglas o estándares específicos que permitan armonizar los tratamientos de datos efectuados por los adheridos, facilitar el ejercicio de los derechos de los afectados y favorecer el cumplimiento de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y el presente reglamento.

2. Los códigos tipo tendrán el carácter de códigos deontológicos o de buena práctica profesional y serán vinculantes para quienes se adhieran a los mismos.

Artículo 72. *Iniciativa y ámbito de aplicación.*

1. Los códigos tipo tendrán carácter voluntario.
2. Los códigos tipo de carácter sectorial podrán referirse a la totalidad o a parte de los tratamientos llevados a cabo por entidades pertenecientes a un mismo sector, debiendo ser formulados por organizaciones representativas de dicho sector, al menos en su ámbito territorial de aplicación, y sin perjuicio de la potestad de dichas entidades de ajustar el código tipo a sus peculiaridades.
3. Los códigos tipo promovidos por una empresa deberán referirse a la totalidad de los tratamientos llevados a cabo por la misma.
4. Las Administraciones públicas y las corporaciones de Derecho Público podrán adoptar códigos tipo de acuerdo con lo establecido en las normas que les sean aplicables.

Artículo 73. *Contenido.*

1. Los códigos tipo deberán estar redactados en términos claros y accesibles.
2. Los códigos tipo deben respetar la normativa vigente e incluir, como mínimo, con suficiente grado de precisión:

a) La delimitación clara y precisa de su ámbito de aplicación, las actividades a que el código se refiere y los tratamientos sometidos al mismo.
b) Las previsiones específicas para la aplicación de los principios de protección de datos.
c) El establecimiento de estándares homogéneos para el cumplimiento por los adheridos al código de las obligaciones establecidas en la Ley Orgánica 15/1999, de 13 de diciembre.
d) El establecimiento de procedimientos que faciliten el ejercicio por los afectados de sus derechos de acceso, rectificación, cancelación y oposición.
e) La determinación de las cesiones y transferencias internacionales de datos que, en su caso, se prevean, con indicación de las garantías que deban adoptarse.
f) Las acciones formativas en materia de protección de datos dirigidas a quienes los traten, especialmente en cuanto a su relación con los afectados.
g) Los mecanismos de supervisión a través de los cuales se garantice el cumplimiento por los adheridos de lo establecido en el código tipo, en los términos previstos en el artículo 74 de este reglamento.

3. En particular, deberán contenerse en el código:
a) Cláusulas tipo para la obtención del consentimiento de los afectados al tratamiento o cesión de sus datos.
b) Cláusulas tipo para informar a los afectados del tratamiento, cuando los datos no sean obtenidos de los mismos.
c) Modelos para el ejercicio por los afectados de sus derechos de acceso, rectificación, cancelación y oposición.
d) Modelos de cláusulas para el cumplimiento de los requisitos formales exigibles para la contratación de un encargado del tratamiento, en su caso.

Artículo 74. *Compromisos adicionales.*

1. Los códigos tipo podrán incluir cualquier otro compromiso adicional que asuman los adheridos para un mejor cumplimiento de la legislación vigente en materia de protección de datos.
2. Además podrán contener cualquier otro compromiso que puedan establecer las entidades promotoras y, en particular, sobre:

a) La adopción de medidas de seguridad adicionales a las exigidas por la Ley Orgánica 15/1999, de 13 de diciembre, y el presente Reglamento.
b) La identificación de las categorías de cesionarios o importadores de los datos.
c) Las medidas concretas adoptadas en materia de protección de los menores o de determinados colectivos de afectados.
d) El establecimiento de un sello de calidad que identifique a los adheridos al código.

Artículo 75. *Garantías del cumplimiento de los códigos tipo.*

1. Los códigos tipo deberán incluir procedimientos de supervisión independientes para garantizar el cumplimiento de las obligaciones asumidas por los adheridos, y establecer un régimen sancionador adecuado, eficaz y disuasorio.

2. El procedimiento que se prevea deberá garantizar:

a) La independencia e imparcialidad del órgano responsable de la supervisión.

b) La sencillez, accesibilidad, celeridad y gratuidad para la presentación de quejas y reclamaciones ante dicho órgano por los eventuales incumplimientos del código tipo.

c) El principio de contradicción.

d) Una graduación de sanciones que permita ajustarlas a la gravedad del incumplimiento. Esas sanciones deberán ser disuasorias y podrán implicar la suspensión de la adhesión al código o la expulsión de la entidad adherida. Asimismo, podrá establecerse, en su caso, su publicidad.

e) La notificación al afectado de la decisión adoptada.

3. Asimismo, y sin perjuicio de lo dispuesto en el artículo 19 de la Ley Orgánica 15/1999, de 13 de diciembre, los códigos tipo podrán contemplar procedimientos para la determinación de medidas reparadoras en caso de haberse causado un perjuicio a los afectados como consecuencia del incumplimiento del código tipo.

4. Lo dispuesto en este artículo se aplicará sin perjuicio de las competencias de la Agencia Española de Protección de Datos y, en su caso, de las autoridades de control de las comunidades autónomas.

Artículo 76. *Relación de adheridos.*

El código tipo deberá incorporar como anexo una relación de adheridos, que deberá mantenerse actualizada, a disposición de la Agencia Española de Protección de Datos.

Artículo 77. *Depósito y publicidad de los códigos tipo.*

1. Para que los códigos tipo puedan ser considerados como tales a los efectos previstos en el artículo 32 de la Ley Orgánica 15/1999, de 13 de diciembre, y el presente reglamento, deberán ser depositados e inscritos en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos o, cuando corresponda, en el registro que fuera creado por las comunidades autónomas, que darán traslado para su inclusión al Registro General de Protección de Datos.

2. A tal efecto, los códigos tipo deberán ser presentados ante la correspondiente autoridad de control, tramitándose su inscripción, en caso de estar sometidos a la decisión de la Agencia Española de Protección de Datos, conforme al procedimiento establecido en el capítulo VI del título IX de este reglamento.

3. En todo caso, la Agencia Española de Protección de Datos dará publicidad a los códigos tipo inscritos, preferentemente a través de medios informáticos o telemáticos.

Artículo 78. *Obligaciones posteriores a la inscripción del código tipo.*

Las entidades promotoras o los órganos, personas o entidades que al efecto se designen en el propio código tipo tendrán, una vez el mismo haya sido publicado, las siguientes obligaciones:

a) Mantener accesible al público la información actualizada sobre las entidades promotoras, el contenido del código tipo, los procedimientos de adhesión y de garantía de su cumplimiento y la relación de adheridos a la que se refiere el artículo anterior.

Esta información deberá presentarse de forma concisa y clara y estar permanentemente accesible por medios electrónicos.

b) Remitir a la Agencia Española de Protección de Datos una memoria anual sobre las actividades realizadas para difundir el código tipo y promover la adhesión a éste, las actuaciones de verificación del cumplimiento del código y sus resultados, las quejas y reclamaciones tramitadas y el curso que se les hubiera dado y cualquier otro aspecto que las entidades promotoras consideren adecuado destacar.

Cuando se trate de códigos tipo inscritos en el registro de una autoridad de control de una comunidad autónoma, la remisión se realizará a dicha autoridad, que dará traslado al registro General de Protección de Datos.

c) Evaluar periódicamente la eficacia del código tipo, midiendo el grado de satisfacción de los afectados y, en su caso, actualizar su contenido para adaptarlo a la normativa general o sectorial de protección de datos existente en cada momento.

Esta evaluación deberá tener lugar, al menos, cada cuatro años, salvo que sea precisa la adaptación de los compromisos del código a la modificación de la normativa aplicable en un plazo menor.

d) Favorecer la accesibilidad de todas las personas, con especial atención a las que tengan alguna discapacidad o de edad avanzada a toda la información disponible sobre el código tipo.

TÍTULO VIII

De las medidas de seguridad en el tratamiento de datos de carácter personal

CAPÍTULO I

Disposiciones generales

Artículo 79. *Alcance.*

Los responsables de los tratamientos o los ficheros y los encargados del tratamiento deberán implantar las medidas de seguridad con arreglo a lo dispuesto en este Título, con independencia de cual sea su sistema de tratamiento.

Artículo 80. *Niveles de seguridad.*

Las medidas de seguridad exigibles a los ficheros y tratamientos se clasifican en tres niveles: básico, medio y alto.

Artículo 81. *Aplicación de los niveles de seguridad.*

1. Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico.

2. Deberán implantarse, además de las medidas de seguridad de nivel básico, las medidas de nivel medio, en los siguientes ficheros o tratamientos de datos de carácter personal:

a) Los relativos a la comisión de infracciones administrativas o penales.

b) Aquellos cuyo funcionamiento se rija por el artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre.

c) Aquellos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias.

d) Aquéllos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros.

e) Aquéllos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias. De igual modo, aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.

f) Aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.

3. Además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán en los siguientes ficheros o tratamientos de datos de carácter personal:

a) Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.

b) Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.
c) Aquéllos que contengan datos derivados de actos de violencia de género.

4. A los ficheros de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización, se aplicarán, además de las medidas de seguridad de nivel básico y medio, la medida de seguridad de nivel alto contenida en el artículo 103 de este reglamento.
5. En caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastará la implantación de las medidas de seguridad de nivel básico cuando:

a) Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros.
b) Se trate de ficheros o tratamientos en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad.

6. También podrán implantarse las medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos.
7. Las medidas incluidas en cada uno de los niveles descritos anteriormente tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes que pudieran resultar de aplicación en cada caso o las que por propia iniciativa adoptase el responsable del fichero.
8. A los efectos de facilitar el cumplimiento de lo dispuesto en este título, cuando en un sistema de información existan ficheros o tratamientos que en función de su finalidad o uso concreto, o de la naturaleza de los datos que contengan, requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad correspondiente y siempre que puedan delimitarse los datos afectados y los usuarios con acceso a los mismos, y que esto se haga constar en el documento de seguridad.

Artículo 82. *Encargado del tratamiento.*

1. Cuando el responsable del fichero o tratamiento facilite el acceso a los datos, a los soportes que los contengan o a los recursos del sistema de información que los trate, a un encargado de tratamiento que preste sus servicios en los locales del primero deberá hacerse constar esta circunstancia en el documento de seguridad de dicho responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.
Cuando dicho acceso sea remoto habiéndose prohibido al encargado incorporar tales datos a sistemas o soportes distintos de los del responsable, este último deberá hacer constar esta circunstancia en el documento de seguridad del responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.
2. Si el servicio fuera prestado por el encargado del tratamiento en sus propios locales, ajenos a los del responsable del fichero, deberá elaborar un documento de seguridad en los términos exigidos por el artículo 88 de este reglamento o completar el que ya hubiera elaborado, en su caso, identificando el fichero o tratamiento y el responsable del mismo e incorporando las medidas de seguridad a implantar en relación con dicho tratamiento.
3. En todo caso, el acceso a los datos por el encargado del tratamiento estará sometido a las medidas de seguridad contempladas en este reglamento.

Artículo 83. *Prestaciones de servicios sin acceso a datos personales.*

El responsable del fichero o tratamiento adoptará las medidas adecuadas para limitar el acceso del personal a datos personales, a los soportes que los contengan o a los recursos

del sistema de información, para la realización de trabajos que no impliquen el tratamiento de datos personales.

Cuando se trate de personal ajeno, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto a los datos que el personal hubiera podido conocer con motivo de la prestación del servicio.

Artículo 84. *Delegación de autorizaciones.*

Las autorizaciones que en este título se atribuyen al responsable del fichero o tratamiento podrán ser delegadas en las personas designadas al efecto. En el documento de seguridad deberán constar las personas habilitadas para otorgar estas autorizaciones así como aquellas en las que recae dicha delegación. En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al responsable del fichero.

Artículo 85. *Acceso a datos a través de redes de comunicaciones.*

Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones, sean o no públicas, deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local, conforme a los criterios establecidos en el artículo 80.

Artículo 86. *Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento.*

1. Cuando los datos personales se almacenen en dispositivos portátiles o se traten fuera de los locales del responsable de fichero o tratamiento, o del encargado del tratamiento será preciso que exista una autorización previa del responsable del fichero o tratamiento, y en todo caso deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

2. La autorización a la que se refiere el párrafo anterior tendrá que constar en el documento de seguridad y podrá establecerse para un usuario o para un perfil de usuarios y determinando un periodo de validez para las mismas.

Artículo 87. *Ficheros temporales o copias de trabajo de documentos.*

1. Aquellos ficheros temporales o copias de documentos que se hubiesen creado exclusivamente para la realización de trabajos temporales o auxiliares deberán cumplir el nivel de seguridad que les corresponda conforme a los criterios establecidos en el artículo 81.

2. Todo fichero temporal o copia de trabajo así creado será borrado o destruido una vez que haya dejado de ser necesario para los fines que motivaron su creación.

CAPÍTULO II

Del documento de seguridad

Artículo 88. *El documento de seguridad.*

1. El responsable del fichero o tratamiento elaborará un documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información.

2. El documento de seguridad podrá ser único y comprensivo de todos los ficheros o tratamientos, o bien individualizado para cada fichero o tratamiento. También podrán elaborarse distintos documentos de seguridad agrupando ficheros o tratamientos según el sistema de tratamiento utilizado para su organización, o bien atendiendo a criterios organizativos del responsable. En todo caso, tendrá el carácter de documento interno de la organización.

3. El documento deberá contener, como mínimo, los siguientes aspectos:

a) Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.

b) Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento.

c) Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.

d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.

e) Procedimiento de notificación, gestión y respuesta ante las incidencias.

f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.

g) Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos.

4. En caso de que fueran de aplicación a los ficheros las medidas de seguridad de nivel medio o las medidas de seguridad de nivel alto, previstas en este título, el documento de seguridad deberá contener además:

a) La identificación del responsable o responsables de seguridad.

b) Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.

5. Cuando exista un tratamiento de datos por cuenta de terceros, el documento de seguridad deberá contener la identificación de los ficheros o tratamientos que se traten en concepto de encargado con referencia expresa al contrato o documento que regule las condiciones del encargo, así como de la identificación del responsable y del período de vigencia del encargo.

6. En aquellos casos en los que datos personales de un fichero o tratamiento se incorporen y traten de modo exclusivo en los sistemas del encargado, el responsable deberá anotarlo en su documento de seguridad. Cuando tal circunstancia afectase a parte o a la totalidad de los ficheros o tratamientos del responsable, podrá delegarse en el encargado la llevanza del documento de seguridad, salvo en lo relativo a aquellos datos contenidos en recursos propios. Este hecho se indicará de modo expreso en el contrato celebrado al amparo del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, con especificación de los ficheros o tratamientos afectados.

En tal caso, se atenderá al documento de seguridad del encargado al efecto del cumplimiento de lo dispuesto por este reglamento.

7. El documento de seguridad deberá mantenerse en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los ficheros o tratamientos o, en su caso, como consecuencia de los controles periódicos realizados. En todo caso, se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.

8. El contenido del documento de seguridad deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

CAPÍTULO III

Medidas de seguridad aplicables a ficheros y tratamientos automatizados

Sección 1.ª Medidas de seguridad de nivel básico

Artículo 89. *Funciones y obligaciones del personal.*

1. Las funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas en el documento de seguridad.

También se definirán las funciones de control o autorizaciones delegadas por el responsable del fichero o tratamiento.

2. El responsable del fichero o tratamiento adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

Artículo 90. *Registro de incidencias.*

Deberá existir un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.

Artículo 91. *Control de acceso.*

1. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.
2. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.
3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.
4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.
5. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

Artículo 92. *Gestión de soportes y documentos.*

1. Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado para ello en el documento de seguridad.

Se exceptúan estas obligaciones cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello en el documento de seguridad.

2. La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del responsable del fichero o tratamiento deberá ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en el documento de seguridad.
3. En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.
4. Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.
5. La identificación de los soportes que contengan datos de carácter personal que la organización considerase especialmente sensibles se podrá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

Artículo 93. *Identificación y autenticación.*

1. El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.
2. El responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.

3. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

4. El documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible.

Artículo 94. *Copias de respaldo y recuperación.*

1. Deberán establecerse procedimientos de actuación para la realización como mínimo semanal de copias de respaldo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

2. Asimismo, se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

Únicamente, en el caso de que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados, y siempre que la existencia de documentación permita alcanzar el objetivo al que se refiere el párrafo anterior, se deberá proceder a grabar manualmente los datos quedando constancia motivada de este hecho en el documento de seguridad.

3. El responsable del fichero se encargará de verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

4. Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado y se anote su realización en el documento de seguridad.

Si está previsto realizar pruebas con datos reales, previamente deberá haberse realizado una copia de seguridad.

Sección 2.ª Medidas de seguridad de nivel medio

Artículo 95. *Responsable de seguridad.*

En el documento de seguridad deberán designarse uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el mismo. Esta designación puede ser única para todos los ficheros o tratamientos de datos de carácter personal o diferenciada según los sistemas de tratamiento utilizados, circunstancia que deberá hacerse constar claramente en el documento de seguridad.

En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde al responsable del fichero o al encargado del tratamiento de acuerdo con este reglamento.

Artículo 96. *Auditoría.*

1. A partir del nivel medio los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título.

Con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas. Esta auditoría inicia el cómputo de dos años señalado en el párrafo anterior.

2. El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.

3. Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero o tratamiento para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas.

Artículo 97. *Gestión de soportes y documentos.*

1. Deberá establecerse un sistema de registro de entrada de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

2. Igualmente, se dispondrá de un sistema de registro de salida de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el destinatario, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.

Artículo 98. *Identificación y autenticación.*

El responsable del fichero o tratamiento establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

Artículo 99. *Control de acceso físico.*

Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información.

Artículo 100. *Registro de incidencias.*

1. En el registro regulado en el artículo 90 deberán consignarse, además, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.

2. Será necesaria la autorización del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos.

Sección 3.ª Medidas de seguridad de nivel alto

Artículo 101. *Gestión y distribución de soportes.*

1. La identificación de los soportes se deberá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

2. La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte.

Asimismo, se cifrarán los datos que contengan los dispositivos portátiles cuando éstos se encuentren fuera de las instalaciones que están bajo el control del responsable del fichero.

3. Deberá evitarse el tratamiento de datos de carácter personal en dispositivos portátiles que no permitan su cifrado. En caso de que sea estrictamente necesario se hará constar motivadamente en el documento de seguridad y se adoptarán medidas que tengan en cuenta los riesgos de realizar tratamientos en entornos desprotegidos.

Artículo 102. *Copias de respaldo y recuperación.*

Deberá conservarse una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los equipos

informáticos que los tratan, que deberá cumplir en todo caso las medidas de seguridad exigidas en este título, o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación.

Artículo 103. *Registro de accesos.*

1. De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.
2. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.
3. Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos.
4. El período mínimo de conservación de los datos registrados será de dos años.
5. El responsable de seguridad se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.
6. No será necesario el registro de accesos definido en este artículo en caso de que concurran las siguientes circunstancias:

a) Que el responsable del fichero o del tratamiento sea una persona física.
b) Que el responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos personales.

La concurrencia de las dos circunstancias a las que se refiere el apartado anterior deberá hacerse constar expresamente en el documento de seguridad.

Artículo 104. *Telecomunicaciones.*

Cuando, conforme al artículo 81.3 deban implantarse las medidas de seguridad de nivel alto, la transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

CAPÍTULO IV

Medidas de seguridad aplicables a los ficheros y tratamientos no automatizados

Sección 1.ª Medidas de seguridad de nivel básico

Artículo 105. *Obligaciones comunes.*

1. Además de lo dispuesto en el presente capítulo, a los ficheros no automatizados les será de aplicación lo dispuesto en los capítulos I y II del presente título en lo relativo a:

a) Alcance.
b) Niveles de seguridad.
c) Encargado del tratamiento.
d) Prestaciones de servicios sin acceso a datos personales.
e) Delegación de autorizaciones.
f) Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento.
g) Copias de trabajo de documentos.
h) Documento de seguridad.

2. Asimismo se les aplicará lo establecido por la sección primera del capítulo III del presente título en lo relativo a:
a) Funciones y obligaciones del personal.

b) Registro de incidencias.
c) Control de acceso.
d) Gestión de soportes.

Artículo 106. *Criterios de archivo.*

El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación. Estos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.

En aquellos casos en los que no exista norma aplicable, el responsable del fichero deberá establecer los criterios y procedimientos de actuación que deban seguirse para el archivo.

Artículo 107. *Dispositivos de almacenamiento.*

Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura. Cuando las características físicas de aquéllos no permitan adoptar esta medida, el responsable del fichero o tratamiento adoptará medidas que impidan el acceso de personas no autorizadas.

Artículo 108. *Custodia de los soportes.*

Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento establecidos en el artículo anterior, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.

Sección 2.ª Medidas de seguridad de nivel medio

Artículo 109. *Responsable de seguridad.*

Se designará uno o varios responsables de seguridad en los términos y con las funciones previstas en el artículo 95 de este reglamento.

Artículo 110. *Auditoría.*

Los ficheros comprendidos en la presente sección se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título.

Sección 3.ª Medidas de seguridad de nivel alto

Artículo 111. *Almacenamiento de la información.*

1. Los armarios, archivadores u otros elementos en los que se almacenen los ficheros no automatizados con datos de carácter personal deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero.

2. Si, atendidas las características de los locales de que dispusiera el responsable del fichero o tratamiento, no fuera posible cumplir lo establecido en el apartado anterior, el responsable adoptará medidas alternativas que, debidamente motivadas, se incluirán en el documento de seguridad.

Artículo 112. *Copia o reproducción.*

1. La generación de copias o la reproducción de los documentos únicamente podrá ser realizada bajo el control del personal autorizado en el documento de seguridad.

2. Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.

Artículo 113. *Acceso a la documentación.*

1. El acceso a la documentación se limitará exclusivamente al personal autorizado.
2. Se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios.
3. El acceso de personas no incluidas en el párrafo anterior deberá quedar adecuadamente registrado de acuerdo con el procedimiento establecido al efecto en el documento de seguridad.

Artículo 114. *Traslado de documentación.*

Siempre que se proceda al traslado físico de la documentación contenida en un fichero, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado.

TÍTULO IX

Procedimientos tramitados por la Agencia Española de Protección de Datos

CAPÍTULO I

Disposiciones generales

Artículo 115. *Régimen aplicable.*

1. Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el presente título, y supletoriamente, por la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.
2. Específicamente serán de aplicación las normas reguladoras del procedimiento administrativo común al régimen de representación en los citados procedimientos.

Artículo 116. *Publicidad de las resoluciones.*

1. La Agencia Española de Protección de Datos hará públicas sus resoluciones, con excepción de las correspondientes a la inscripción de un fichero o tratamiento en el Registro General de Protección de Datos y de aquéllas por las que se resuelva la inscripción en el mismo de los códigos tipo, siempre que se refieran a procedimientos que se hubieran iniciado con posterioridad al 1 de enero de 2004, o correspondan al archivo de actuaciones inspectoras incoadas a partir de dicha fecha.
2. La publicación de estas resoluciones se realizará preferentemente mediante su inserción en el sitio web de la Agencia Española de Protección de Datos, dentro del plazo de un mes a contar desde la fecha de su notificación a los interesados.
3. En la notificación de las resoluciones se informará expresamente a los interesados de la publicidad prevista en el artículo 37.2 de la Ley Orgánica 15/1999, de 13 de diciembre.
4. La publicación se realizará aplicando los criterios de disociación de los datos de carácter personal que a tal efecto se establezcan mediante Resolución del Director de la Agencia.

CAPÍTULO II

Procedimiento de tutela de los derechos de acceso, rectificación, cancelación y oposición

Artículo 117. *Instrucción del procedimiento.*

1. El procedimiento se iniciará a instancia del afectado o afectados, expresando con claridad el contenido de su reclamación y de los preceptos de la Ley Orgánica 15/1999, de 13 de diciembre, que se consideran vulnerados.

2. Recibida la reclamación en la Agencia Española de Protección de Datos, se dará traslado de la misma al responsable del fichero, para que, en el plazo de quince días, formule las alegaciones que estime pertinentes.

3. Recibidas las alegaciones o transcurrido el plazo previsto en el apartado anterior, la Agencia Española de Protección de Datos, previos los informes, pruebas y otros actos de instrucción pertinentes, incluida la audiencia del afectado y nuevamente del responsable del fichero, resolverá sobre la reclamación formulada.

Artículo 118. *Duración del procedimiento y efectos de la falta de resolución expresa.*

1. El plazo máximo para dictar y notificar resolución en el procedimiento de tutela de derechos será de seis meses, a contar desde la fecha de entrada en la Agencia Española de Protección de Datos de la reclamación del afectado o afectados.

2. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, el afectado podrá considerar estimada su reclamación por silencio administrativo positivo.

Artículo 119. *Ejecución de la resolución.*

Si la resolución de tutela fuese estimatoria, se requerirá al responsable del fichero para que, en el plazo de diez días siguientes a la notificación, haga efectivo el ejercicio de los derechos objeto de la tutela, debiendo dar cuenta por escrito de dicho cumplimiento a la Agencia Española de Protección de Datos en idéntico plazo.

CAPÍTULO III

Procedimientos relativos al ejercicio de la potestad sancionadora

Sección 1.ª Disposiciones generales

Artículo 120. *Ámbito de aplicación.*

1. Las disposiciones contenidas en el presente capítulo serán de aplicación a los procedimientos relativos al ejercicio por la Agencia Española de Protección de Datos de la potestad sancionadora que le viene atribuida por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal, en la Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico, y en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

2. No obstante, las disposiciones previstas en el ar-tículo 121 y en la sección cuarta de este capítulo únicamente serán aplicables a los procedimientos referidos al ejercicio de la potestad sancionadora prevista en la Ley Orgánica 15/1999, de 13 de diciembre.

Artículo 121. *Inmovilización de ficheros.*

1. En el supuesto previsto como infracción muy grave en la Ley Orgánica 15/1999, de 13 de diciembre, consistente en la utilización o cesión ilícita de los datos de carácter personal en la que se impida gravemente o se atente de igual modo contra el ejercicio de los derechos de los ciudadanos y el libre desarrollo de la personalidad que la Constitución y las leyes garantizan, el Director de la Agencia Española de Protección de Datos podrá, en cualquier momento del procedimiento, requerir a los responsables de ficheros o tratamientos de datos de carácter personal, tanto de titularidad pública como privada, la cesación en la utilización o cesión ilícita de los datos.

2. El requerimiento deberá ser atendido en el plazo improrrogable de tres días, durante el cual el responsable del fichero podrá formular las alegaciones que tenga por convenientes en orden al levantamiento de la medida.

3. Si el requerimiento fuera desatendido, el Director de la Agencia Española de Protección de Datos podrá, mediante resolución motivada, acordar la inmovilización de tales ficheros o tratamientos, a los solos efectos de restaurar los derechos de las personas afectadas.

Sección 2.ª Actuaciones previas

Artículo 122. *Iniciación.*

1. Con anterioridad a la iniciación del procedimiento sancionador, se podrán realizar actuaciones previas con objeto de determinar si concurren circunstancias que justifiquen tal iniciación. En especial, estas actuaciones se orientarán a determinar, con la mayor precisión posible, los hechos que pudieran justificar la incoación del procedimiento, identificar la persona u órgano que pudiera resultar responsable y fijar las circunstancias relevantes que pudieran concurrir en el caso.

2. Las actuaciones previas se llevarán a cabo de oficio por la Agencia Española de Protección de Datos, bien por iniciativa propia o como consecuencia de la existencia de una denuncia o una petición razonada de otro órgano.

3. Cuando las actuaciones se lleven a cabo como consecuencia de la existencia de una denuncia o de una petición razonada de otro órgano, la Agencia Española de Protección de Datos acusará recibo de la denuncia o petición, pudiendo solicitar cuanta documentación se estime oportuna para poder comprobar los hechos susceptibles de motivar la incoación del procedimiento sancionador.

4. Estas actuaciones previas tendrán una duración máxima de doce meses a contar desde la fecha en la que la denuncia o petición razonada a las que se refiere el apartado 2 hubieran tenido entrada en la Agencia Española de Protección de Datos o, en caso de no existir aquéllas, desde que el Director de la Agencia acordase la realización de dichas actuaciones.

El vencimiento del plazo sin que haya sido dictado y notificado acuerdo de inicio de procedimiento sancionador producirá la caducidad de las actuaciones previas.

Artículo 123. *Personal competente para la realización de las actuaciones previas.*

1. Las actuaciones previas serán llevadas a cabo por el personal del área de la Inspección de Datos habilitado para el ejercicio de funciones inspectoras.

2. **(Anulado)**

3. Los funcionarios que ejerzan la inspección a los que se refieren los dos apartados anteriores tendrán la consideración de autoridad pública en el desempeño de sus cometidos.

Estarán obligados a guardar secreto sobre las informaciones que conozcan en el ejercicio de las mencionadas funciones, incluso después de haber cesado en las mismas.

Artículo 124. *Obtención de información.*

Los inspectores podrán recabar cuantas informaciones precisen para el cumplimiento de sus cometidos. A tal fin podrán requerir la exhibición o el envío de los documentos y datos y examinarlos en el lugar en que se encuentren depositados, como obtener copia de los mismos, inspeccionar los equipos físicos y lógicos, así como requerir la ejecución de tratamientos y programas o procedimientos de gestión y soporte del fichero o ficheros sujetos a investigación, accediendo a los lugares donde se hallen instalados.

Artículo 125. *Actuaciones presenciales.*

1. En el desarrollo de las actuaciones previas se podrán realizar visitas de inspección por parte de los inspectores designados, en los locales o sede del inspeccionado, o donde se encuentren ubicados los ficheros, en su caso. A tal efecto, los inspectores habrán sido previamente autorizados por el Director de la Agencia Española de Protección de Datos.

Las inspecciones podrán realizarse en el domicilio del inspeccionado, en la sede o local concreto relacionado con el mismo o en cualquiera de sus locales, incluyendo aquéllos en que el tratamiento sea llevado a cabo por un encargado.

La autorización se limitará a indicar la habilitación del inspector autorizado y la identificación de la persona u órgano inspeccionado.

2. En el supuesto contemplado en el apartado anterior, las inspecciones concluirán con el levantamiento de la correspondiente acta, en la que quedará constancia de las actuaciones practicadas durante la visita o visitas de inspección.

3. El acta, que se emitirá por duplicado, será firmada por los inspectores actuantes y por el inspeccionado, que podrá hacer constar en la misma las alegaciones o manifestaciones que tenga por conveniente.

En caso de negativa del inspeccionado a la firma del acta, se hará constar expresamente esta circunstancia en la misma. En todo caso, la firma por el inspeccionado del acta no supondrá su conformidad, sino tan sólo la recepción de la misma.

Se entregará al inspeccionado uno de los originales del acta de inspección, incorporándose el otro a las actuaciones.

Artículo 126. *Resultado de las actuaciones previas.*

1. Finalizadas las actuaciones previas, éstas se someterán a la decisión del Director de la Agencia Española de Protección de Datos.

Si de las actuaciones no se derivasen hechos susceptibles de motivar la imputación de infracción alguna, el Director de la Agencia Española de Protección de Datos dictará resolución de archivo que se notificará al investigado y al denunciante, en su caso.

2. En caso de apreciarse la existencia de indicios susceptibles de motivar la imputación de una infracción, el Director de la Agencia Española de Protección de Datos dictará acuerdo de inicio de procedimiento sancionador o de infracción de las Administraciones públicas, que se tramitarán conforme a lo dispuesto, respectivamente, en las secciones tercera y cuarta del presente capítulo.

Sección 3.ª Procedimiento sancionador

Artículo 127. *Iniciación del procedimiento.*

Con carácter específico el acuerdo de inicio del procedimiento sancionador deberá contener:

a) Identificación de la persona o personas presuntamente responsables.

b) Descripción sucinta de los hechos imputados, su posible calificación y las sanciones que pudieran corresponder, sin perjuicio de lo que resulte de la instrucción.

c) Indicación de que el órgano competente para resolver el procedimiento es el Director de la Agencia Española de Protección de Datos.

d) Indicación al presunto responsable de que puede reconocer voluntariamente su responsabilidad, en cuyo caso se dictará directamente resolución.

e) Designación de instructor y, en su caso, secretario, con expresa indicación del régimen de recusación de los mismos.

f) Indicación expresa del derecho del responsable a formular alegaciones, a la audiencia en el procedimiento y a proponer las pruebas que estime procedentes.

g) Medidas de carácter provisional que pudieran acordarse, en su caso, conforme a lo establecido en la sección primera del presente capítulo.

Artículo 128. *Plazo máximo para resolver.*

1. El plazo para dictar resolución será el que determinen las normas aplicables a cada procedimiento sancionador y se computará desde la fecha en que se dicte el acuerdo de inicio hasta que se produzca la notificación de la resolución sancionadora, o se acredite debidamente el intento de notificación.

2. El vencimiento del citado plazo máximo, sin que se haya dictada y notificada resolución expresa, producirá la caducidad del procedimiento y el archivo de las actuaciones.

Sección 4.ª Procedimiento de declaración de infracción de la Ley Orgánica 15/1999, de 13 de diciembre, por las administraciones públicas

Artículo 129. *Disposición general.*

El procedimiento por el que se declare la existencia de una infracción de la Ley Orgánica 15/1999, de 13 de diciembre, cometida por las Administraciones públicas será el establecido en la sección tercera de este capítulo.

CAPÍTULO IV

Procedimientos relacionados con la inscripción o cancelación de ficheros

Sección 1.ª Procedimiento de inscripción de la creación, modificación o supresión de ficheros

Artículo 130. *Iniciación del procedimiento.*

1. El procedimiento se iniciará como consecuencia de la notificación de la creación, modificación o supresión del fichero por el interesado o, en su caso, de la comunicación efectuada por las autoridades de control de las comunidades autónomas, a la que se refiere el presente reglamento.

2. La notificación se deberá efectuar cumplimentando los modelos o formularios electrónicos publicados al efecto por la Agencia Española de Protección de Datos, en virtud de lo dispuesto en el apartado 1 del artículo 59 de este reglamento.

Tratándose de la notificación de la modificación o supresión de un fichero, deberá indicarse en la misma el código de inscripción del fichero en el Registro General de Protección de Datos.

3. La notificación se efectuará en soporte electrónico, ya mediante comunicación electrónica a través de Internet mediante firma electrónica o en soporte informático, utilizando al efecto el programa de ayuda para la generación de notificaciones que la Agencia pondrá a disposición de los interesados de forma gratuita.

Será igualmente válida la notificación efectuada en soporte papel cuando para su cumplimentación hayan sido utilizados los modelos o formularios publicados por la Agencia.

4. En la notificación, el responsable del fichero deberá declarar un domicilio a efectos de notificaciones en el procedimiento.

Artículo 131. *Especialidades en la notificación de ficheros de titularidad pública.*

1. Cuando se trate de la notificación de ficheros de titularidad pública, deberá acompañarse a la notificación una copia de la norma o acuerdo de creación, modificación o supresión del fichero a que hace referencia el ar-tículo 52 del presente reglamento.

Cuando el diario oficial en el que se encuentre publicada la citada norma o acuerdo sea accesible a través de Internet, bastará con indicar en la notificación la dirección electrónica que permita su concreta localización.

2. Recibida la notificación, si la misma no contuviera la información preceptiva o se advirtieran defectos formales, el Registro General de Protección de Datos requerirá al responsable del fichero para que complete o subsane la notificación. El plazo para la subsanación o mejora de la solicitud será de tres meses, en el caso de que se precise la modificación de la norma o acuerdo de creación del fichero.

Artículo 132. *Acuerdo de inscripción o cancelación.*

Si la notificación referida a la creación, modificación o supresión del fichero contuviera la información preceptiva y se cumplieran las restantes exigencias legales, el Director de la Agencia Española de Protección de Datos, a propuesta del Registro General de Protección de Datos, acordará, respectivamente, la inscripción del fichero, asignando al mismo el correspondiente código de inscripción, la modificación de la inscripción del fichero o la cancelación de la inscripción correspondiente.

Artículo 133. *Improcedencia o denegación de la inscripción.*

El Director de la Agencia Española de Protección de Datos, a propuesta del Registro General de Protección de Datos, dictará resolución denegando la inscripción, modificación o cancelación cuando de los documentos aportados por el responsable del fichero se desprenda que la notificación no resulta conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre.

La resolución será debidamente motivada, con indicación expresa de las causas que impiden la inscripción, modificación o cancelación.

Artículo 134. *Duración del procedimiento y efectos de la falta de resolución expresa.*

1. El plazo máximo para dictar y notificar resolución acerca de la inscripción, modificación o cancelación será de un mes.
2. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, se entenderá inscrito, modificado o cancelado el fichero a todos los efectos.

Sección 2.ª Procedimiento de cancelación de oficio de ficheros inscritos

Artículo 135. *Iniciación del procedimiento.*

El procedimiento de cancelación de oficio de los ficheros inscritos en el Registro General de Protección de Datos se iniciará siempre de oficio, bien por propia iniciativa o en virtud de denuncia, por acuerdo del Director de la Agencia Española de Protección de Datos.

Artículo 136. *Terminación del expediente.*

La resolución, previa audiencia del interesado, acordará haber lugar o no a la cancelación del fichero.
Si la resolución acordase la cancelación del fichero, se dará traslado de la misma al Registro General de Protección de Datos, para que proceda a la cancelación.

CAPÍTULO V

Procedimientos relacionados con las transferencias internacionales de datos

Sección 1.ª Procedimiento de autorización de transferencias internacionales de datos

Artículo 137. *Iniciación del procedimiento.*

1. El procedimiento para la obtención de la autorización para las transferencias internacionales de datos a países terceros a las que se refiere el artículo 33 de la Ley Orgánica 15/1999, de 13 de diciembre, y el artículo 70 de este reglamento se iniciará siempre a solicitud del exportador que pretenda llevar a cabo la transferencia.
2. En su solicitud, además de los requisitos legalmente exigidos, el exportador deberá consignar, en todo caso:

a) La identificación del fichero o ficheros a cuyos datos se refiera la transferencia internacional, con indicación de su denominación y código de inscripción del fichero en el Registro General de Protección de Datos.
b) La transferencia o transferencias respecto de las que se solicita la autorización, con indicación de la finalidad que la justifica.
c) La documentación que incorpore las garantías exigibles para la obtención de la autorización así como el cumplimiento de los requisitos legales necesarios para la realización de la transferencia, en su caso.

Cuando la autorización se fundamente en la existencia de un contrato entre el exportador y el importador de los datos, deberá aportarse copia del mismo, acreditándose asimismo la concurrencia de poder suficiente en sus otorgantes.
Si la autorización se pretendiera fundar en lo dispuesto en el apartado 4 del artículo 70, deberán aportarse las normas o reglas adoptadas en relación con el tratamiento de los datos en el seno del grupo, así como la documentación que acredite su carácter vinculante y su eficacia dentro del grupo. Igualmente deberá aportarse la documentación que acredite la posibilidad de que el afectado o la Agencia Española de Protección de Datos puedan exigir la responsabilidad que corresponda en caso de perjuicio del afectado o vulneración de las normas de protección de datos por parte de cualquier empresa importadora.

Artículo 138. *Instrucción del procedimiento.*

1. Cuando el Director de la Agencia Española de Protección de Datos acuerde, conforme a lo dispuesto en el artículo 86.1 de la Ley 30/1992, de 26 de noviembre, la apertura de un

período de información pública, el plazo para la formulación de alegaciones será de diez días a contar desde la publicación en el «Boletín Oficial del Estado» del anuncio previsto en dicha Ley.

2. No será posible el acceso a la información del expediente en que concurran las circunstancias establecidas en el artículo 37.5 de la Ley 30/1992, de 26 de noviembre.

3. Transcurrido el plazo previsto en el apartado 1, en caso de que se hubieran formulado alegaciones, se dará traslado de las mismas al solicitante de la autorización, a fin de que en el plazo de diez días alegue lo que estime procedente.

Artículo 139. *Actos posteriores a la resolución.*

1. Cuando el Director de la Agencia Española de Protección de Datos resuelva autorizar la transferencia internacional de datos, se dará traslado de la resolución de autorización al Registro General de Protección de Datos, a fin de proceder a su inscripción.

El Registro General de Protección de Datos inscribirá de oficio la autorización de transferencia internacional.

2. En todo caso, se dará traslado de la resolución de autorización o denegación de la autorización de la transferencia internacional de datos al Ministerio de Justicia, al efecto de que se proceda a su notificación a la Comisión Europea y a los demás Estados miembros de la Unión Europea de acuerdo a lo previsto en el artículo 26.3 de la Directiva 95/46/CE.

Artículo 140. *Duración del procedimiento y efectos de la falta de resolución expresa.*

1. El plazo máximo para dictar y notificar resolución será de tres meses, a contar desde la fecha de entrada en la Agencia Española de Protección de Datos de la solicitud.

2. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, se entenderá autorizada la transferencia internacional de datos.

Sección 2.ª Procedimiento de suspensión temporal de transferencias internacionales de datos

Artículo 141. *Iniciación.*

1. En los supuestos contemplados en el artículo 69 y en el apartado 3 del artículo 70, el Director de la Agencia Española de Protección de Datos podrá acordar la suspensión temporal de una transferencia internacional de datos.

2. En tales supuestos, el Director dictará acuerdo de inicio referido a la suspensión temporal de la transferencia. El acuerdo deberá ser motivado y fundarse en los supuestos previstos en este reglamento.

Artículo 142. *Instrucción y resolución.*

1. Se dará traslado del acuerdo al exportador, a fin de que en el plazo de quince días formule lo que a su derecho convenga.

2. Recibidas las alegaciones o cumplido el plazo señalado, el Director dictará resolución acordando, en su caso, la suspensión temporal de la transferencia internacional de datos.

Artículo 143. *Actos posteriores a la resolución.*

1. El Director de la Agencia Española de Protección de Datos dará traslado de la resolución al Registro General de Protección de Datos, a fin de que la misma se haga constar en el registro.

El Registro General de Protección de Datos inscribirá de oficio la suspensión temporal de la transferencia internacional.

2. En todo caso, se dará traslado de la resolución al Ministerio de Justicia, al efecto de que se proceda a su notificación a la Comisión Europea y a los demás Estados miembros de la Unión Europea de acuerdo a lo previsto en el artículo 26.3 de la Directiva 95/46/CE.

Artículo 144. *Levantamiento de la suspensión temporal.*

1. La suspensión se levantará tan pronto como cesen las causas que la hubieran justificado, mediante resolución del Director de la Agencia Española de Protección de Datos, del que se dará traslado al exportador.

2. El Director de la Agencia Española de Protección de Datos dará traslado de la resolución al Registro General de Protección de Datos, a fin de que la misma se haga constar en el Registro.

El Registro General de Protección de Datos hará constar de oficio el levantamiento de la suspensión temporal de la transferencia internacional.

3. El acuerdo será notificado al exportador y al Ministerio de Justicia, al efecto de que se proceda a su notificación a la Comisión Europea y a los demás Estados miembros de la Unión Europea de acuerdo a lo previsto en el artículo 26. 3 de la Directiva 95/46/CE.

CAPÍTULO VI

Procedimiento de inscripción de códigos tipo

Artículo 145. *Iniciación del procedimiento.*

1. El procedimiento para la inscripción en el Registro General de Protección de Datos de los códigos tipo se iniciará siempre a solicitud de la entidad, órgano o asociación promotora del código tipo.

2. La solicitud, que deberá reunir los requisitos legalmente establecidos, habrá de acompañarse de los siguientes documentos:

a) Acreditación de la representación que concurra en la persona que presente la solicitud.

b) Contenido del acuerdo, convenio o decisión por la que se aprueba, en el ámbito correspondiente el contenido del código tipo presentado.

c) En caso de que el código tipo proceda de un acuerdo sectorial o una decisión de empresa certificación referida a la adopción del acuerdo y legitimación del órgano que lo adoptó.

d) En el supuesto contemplado en la letra anterior, copia de los estatutos de la asociación, organización sectorial o entidad en cuyo marco haya sido aprobado el código.

e) En caso de códigos tipo presentados por asociaciones u organizaciones de carácter sectorial, documentación relativa a su representatividad en el sector.

f) En caso de códigos tipo basados en decisiones de empresa, descripción de los tratamientos a los que se refiere el código tipo.

g) Código tipo sometido a la Agencia Española de Protección de Datos.

Artículo 146. *Análisis de los aspectos sustantivos del código tipo.*

1. Durante los treinta días siguientes a la notificación o subsanación de los defectos el Registro General de Protección de Datos podrá convocar a los solicitantes, a fin de obtener aclaraciones o precisiones relativas al contenido sustantivo del código tipo.

2. Transcurrido el plazo señalado en el apartado anterior, el Registro General de Protección de Datos elaborará un informe sobre las características del proyecto de código tipo.

3. La documentación presentada y el informe del Registro serán remitidos al Gabinete Jurídico, a fin de que por el mismo se informe acerca del cumplimiento de los requisitos establecidos en el Título VII de este Reglamento.

Artículo 147. *Información pública.*

1. Cuando el Director de la Agencia Española de Protección de Datos acuerde, conforme a lo dispuesto en el artículo 86.1 de la Ley 30/1992, de 26 de noviembre, la apertura de un período de información pública, el plazo para la formulación de alegaciones será de diez días a contar desde la publicación en el «Boletín Oficial del Estado» del anuncio previsto en dicha ley.

2. No será posible el acceso a la información del expediente en que concurran las circunstancias establecidas en el artículo 37.5 de la Ley 30/1992, de 26 de noviembre.

Artículo 148. *Mejora del código tipo.*

Si durante la tramitación del procedimiento resultase necesaria la aportación de nuevos documentos o la modificación del código tipo presentado, la Agencia Española de Protección de Datos podrá requerir al solicitante, a fin de que en el plazo de treinta días introduzca las modificaciones que sean precisas, remitiendo el texto resultante a la Agencia Española de Protección de Datos.

Se declarará la suspensión del procedimiento en tanto el solicitante no dé cumplimiento al requerimiento.

Artículo 149. *Trámite de audiencia.*

En caso de que durante el trámite previsto en el ar-tículo 148 se hubieran formulado alegaciones, se dará traslado de las mismas al solicitante de la autorización, a fin de que en el plazo de diez días alegue lo que estime procedente.

Artículo 150. *Resolución.*

1. Cumplidos los términos establecidos en los artículos precedentes, el Director de la Agencia resolverá sobre la procedencia o improcedencia de la inscripción del código tipo en el Registro General de Protección de Datos.

2. Cuando el Director de la Agencia Española de Protección de Datos resuelva autorizar la inscripción del código tipo, se dará traslado de la resolución al Registro General de Protección de Datos, a fin de proceder a su inscripción.

Artículo 151. *Duración del procedimiento y efectos de la falta de resolución expresa.*

1. El plazo máximo para dictar y notificar resolución será de seis meses, a contar desde la fecha de entrada de la solicitud en la Agencia Española de Protección de Datos.

2. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, el solicitante podrá considerar estimada su solicitud.

Artículo 152. *Publicación de los códigos tipo por la Agencia Española de Protección de Datos.*

La Agencia Española de Protección de Datos dará publicidad al contenido de los códigos tipo inscritos en el Registro General de Protección de Datos, utilizando para ello, con carácter preferente, medios electrónicos o telemáticos.

CAPÍTULO VII

Otros procedimientos tramitados por la agencia española de protección de datos

Sección 1.ª Procedimiento de exención del deber de información al interesado

Artículo 153. *Iniciación del procedimiento.*

1. El procedimiento para obtener de la Agencia Española de Protección de Datos la exención del deber de informar al interesado acerca del tratamiento de sus datos de carácter personal cuando resulte imposible o exija esfuerzos desproporcionados, prevista en el apartado 5 del artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, se iniciará siempre a petición del responsable que pretenda obtener la aplicación de la exención.

2. En el escrito de solicitud, además de los requisitos recogidos en el art. 70 de la Ley 30/1992, de 26 de noviembre, el responsable deberá:

a) Identificar claramente el tratamiento de datos al que pretende aplicarse la exención del deber de informar.

b) Motivar expresamente las causas en que fundamenta la imposibilidad o el carácter desproporcionado del esfuerzo que implicaría el cumplimiento del deber de informar.

c) Exponer detalladamente las medidas compensatorias que propone realizar en caso de exoneración del cumplimiento del deber de informar.

d) Aportar una cláusula informativa que, mediante su difusión, en los términos que se indiquen en la solicitud, permita compensar la exención del deber de informar.

Artículo 154. *Propuesta de nuevas medidas compensatorias.*

1. Si la Agencia Española de Protección de Datos considerase insuficientes las medidas compensatorias propuestas por el solicitante, podrá acordar la adopción de medidas complementarias o sustitutivas a las propuestas por aquél en su solicitud.

2. Del acuerdo se dará traslado al solicitante, a fin de que exponga lo que a su derecho convenga en el plazo de quince días.

Artículo 155. *Terminación del procedimiento.*

Concluidos los trámites previstos en los artículos precedentes, el Director de la Agencia dictará resolución, concediendo o denegando la exención del deber de informar. La resolución podrá imponer la adopción de las medidas complementarias a las que se refiere el artículo anterior.

Artículo 156. *Duración del procedimiento y efectos de la falta de resolución expresa.*

1. El plazo máximo para dictar y notificar resolución en el procedimiento será de seis meses, a contar desde la fecha de entrada en la Agencia Española de Protección de Datos de la solicitud del responsable del fichero.

2. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, el afectado podrá considerar estimada su solicitud por silencio administrativo positivo.

Sección 2.ª Procedimiento para la autorización de conservación de datos para fines históricos, estadísticos o científicos

Artículo 157. *Iniciación del procedimiento.*

1. El procedimiento para obtener de la Agencia Española de Protección de Datos la declaración de la concurrencia en un determinado tratamiento de datos de valores históricos, científicos o estadísticos, a los efectos previstos en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente Reglamento, se iniciará siempre a petición del responsable que pretenda obtener la declaración.

2. En el escrito de solicitud, el responsable deberá:

a) Identificar claramente el tratamiento de datos al que pretende aplicarse la excepción.

b) Motivar expresamente las causas que justificarían la declaración.

c) Exponer detalladamente las medidas que el responsable del fichero se propone implantar para garantizar el derecho de los ciudadanos.

3. La solicitud deberá acompañarse de cuantos documentos o pruebas sean necesarios para justificar la existencia de los valores históricos, científicos o estadísticos que fundamentarían la declaración de la Agencia.

Artículo 158. *Duración del procedimiento y efectos de la falta de resolución expresa.*

1. El plazo máximo para dictar y notificar resolución en el procedimiento será de tres meses, a contar desde la fecha de entrada en la Agencia Española de Protección de Datos de la solicitud del responsable del fichero.

2. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, el afectado podrá considerar estimada su solicitud.

Disposición adicional única. *Productos de software.*

Los productos de software destinados al tratamiento automatizado de datos personales deberán incluir en su descripción técnica el nivel de seguridad, básico, medio o alto, que permitan alcanzar de acuerdo con lo establecido en el título VIII de este reglamento.

Disposición final única. *Aplicación supletoria.*

En lo no establecido en el capítulo III del título IX serán de aplicación a los procedimientos sancionadores tramitados por la Agencia Española de Protección de Datos las disposiciones contenidas en el Reglamento del Procedimiento para el ejercicio de la potestad sancionadora, aprobado por Real Decreto 1398/1993, de 4 de agosto.

§ 53

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

Unión Europea
«DOUE» núm. 119, de 4 de mayo de 2016
Última modificación: sin modificaciones
Referencia: DOUE-L-2016-89807

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea, y en particular su artículo 16,

Vista la propuesta de la Comisión Europea,

Previa transmisión del proyecto de texto legislativo a los Parlamentos nacionales,

Visto el dictamen del Comité Económico y Social Europeo [1],

Visto el dictamen del Comité de las Regiones [2],

De conformidad con el procedimiento legislativo ordinario [3],

Considerando lo siguiente:

(1) La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental. El artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea («la Carta») y el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE) establecen que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

(2) Los principios y normas relativos a la protección de las personas físicas en lo que respecta al tratamiento de sus datos de carácter personal deben, cualquiera que sea su nacionalidad o residencia, respetar sus libertades y derechos fundamentales, en particular el derecho a la protección de los datos de carácter personal. El presente Reglamento pretende contribuir a la plena realización de un espacio de libertad, seguridad y justicia y de una unión económica, al progreso económico y social, al refuerzo y la convergencia de las economías dentro del mercado interior, así como al bienestar de las personas físicas.

(3) La Directiva 95/46/CE del Parlamento Europeo y del Consejo [4] trata de armonizar la protección de los derechos y las libertades fundamentales de las personas físicas en relación con las actividades de tratamiento de datos de carácter personal y garantizar la libre circulación de estos datos entre los Estados miembros.

(4) El tratamiento de datos personales debe estar concebido para servir a la humanidad. El derecho a la protección de los datos personales no es un derecho absoluto sino que debe

considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad. El presente Reglamento respeta todos los derechos fundamentales y observa las libertades y los principios reconocidos en la Carta conforme se consagran en los Tratados, en particular el respeto de la vida privada y familiar, del domicilio y de las comunicaciones, la protección de los datos de carácter personal, la libertad de pensamiento, de conciencia y de religión, la libertad de expresión y de información, la libertad de empresa, el derecho a la tutela judicial efectiva y a un juicio justo, y la diversidad cultural, religiosa y lingüística.

(5) La integración económica y social resultante del funcionamiento del mercado interior ha llevado a un aumento sustancial de los flujos transfronterizos de datos personales. En toda la Unión se ha incrementado el intercambio de datos personales entre los operadores públicos y privados, incluidas las personas físicas, las asociaciones y las empresas. El Derecho de la Unión insta a las autoridades nacionales de los Estados miembros a que cooperen e intercambien datos personales a fin de poder cumplir sus funciones o desempeñar otras por cuenta de una autoridad de otro Estado miembro.

(6) La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. La tecnología ha transformado tanto la economía como la vida social, y ha de facilitar aún más la libre circulación de datos personales dentro de la Unión y la transferencia a terceros países y organizaciones internacionales, garantizando al mismo tiempo un elevado nivel de protección de los datos personales.

(7) Estos avances requieren un marco más sólido y coherente para la protección de datos en la Unión Europea, respaldado por una ejecución estricta, dada la importancia de generar la confianza que permita a la economía digital desarrollarse en todo el mercado interior. Las personas físicas deben tener el control de sus propios datos personales. Hay que reforzar la seguridad jurídica y práctica para las personas físicas, los operadores económicos y las autoridades públicas.

(8) En los casos en que el presente Reglamento establece que sus normas sean especificadas o restringidas por el Derecho de los Estados miembros, estos, en la medida en que sea necesario por razones de coherencia y para que las disposiciones nacionales sean comprensibles para sus destinatarios, pueden incorporar a su Derecho nacional elementos del presente Reglamento.

(9) Aunque los objetivos y principios de la Directiva 95/46/CE siguen siendo válidos, ello no ha impedido que la protección de los datos en el territorio de la Unión se aplique de manera fragmentada, ni la inseguridad jurídica ni una percepción generalizada entre la opinión pública de que existen riesgos importantes para la protección de las personas físicas, en particular en relación con las actividades en línea. Las diferencias en el nivel de protección de los derechos y libertades de las personas físicas, en particular del derecho a la protección de los datos de carácter personal, en lo que respecta al tratamiento de dichos datos en los Estados miembros pueden impedir la libre circulación de los datos de carácter personal en la Unión. Estas diferencias pueden constituir, por lo tanto, un obstáculo al ejercicio de las actividades económicas a nivel de la Unión, falsear la competencia e impedir que las autoridades cumplan las funciones que les incumben en virtud del Derecho de la Unión. Esta diferencia en los niveles de protección se debe a la existencia de divergencias en la ejecución y aplicación de la Directiva 95/46/CE.

(10) Para garantizar un nivel uniforme y elevado de protección de las personas físicas y eliminar los obstáculos a la circulación de datos personales dentro de la Unión, el nivel de protección de los derechos y libertades de las personas físicas por lo que se refiere al tratamiento de dichos datos debe ser equivalente en todos los Estados miembros. Debe garantizarse en toda la Unión que la aplicación de las normas de protección de los derechos y libertades fundamentales de las personas físicas en relación con el tratamiento de datos de carácter personal sea coherente y homogénea. En lo que respecta al tratamiento de datos personales para el cumplimiento de una obligación legal, para el cumplimiento de una misión

realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, los Estados miembros deben estar facultados para mantener o adoptar disposiciones nacionales a fin de especificar en mayor grado la aplicación de las normas del presente Reglamento. Junto con la normativa general y horizontal sobre protección de datos por la que se aplica la Directiva 95/46/CE, los Estados miembros cuentan con distintas normas sectoriales específicas en ámbitos que precisan disposiciones más específicas. El presente Reglamento reconoce también un margen de maniobra para que los Estados miembros especifiquen sus normas, inclusive para el tratamiento de categorías especiales de datos personales («datos sensibles»). En este sentido, el presente Reglamento no excluye el Derecho de los Estados miembros que determina las circunstancias relativas a situaciones específicas de tratamiento, incluida la indicación pormenorizada de las condiciones en las que el tratamiento de datos personales es lícito.

(11) La protección efectiva de los datos personales en la Unión exige que se refuercen y especifiquen los derechos de los interesados y las obligaciones de quienes tratan y determinan el tratamiento de los datos de carácter personal, y que en los Estados miembros se reconozcan poderes equivalentes para supervisar y garantizar el cumplimiento de las normas relativas a la protección de los datos de carácter personal y las infracciones se castiguen con sanciones equivalentes.

(12) El artículo 16, apartado 2, del TFUE encomienda al Parlamento Europeo y al Consejo que establezcan las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal y las normas relativas a la libre circulación de dichos datos.

(13) Para garantizar un nivel coherente de protección de las personas físicas en toda la Unión y evitar divergencias que dificulten la libre circulación de datos personales dentro del mercado interior, es necesario un reglamento que proporcione seguridad jurídica y transparencia a los operadores económicos, incluidas las microempresas y las pequeñas y medianas empresas, y ofrezca a las personas físicas de todos los Estados miembros el mismo nivel de derechos y obligaciones exigibles y de responsabilidades para los responsables y encargados del tratamiento, con el fin de garantizar una supervisión coherente del tratamiento de datos personales y sanciones equivalentes en todos los Estados miembros, así como la cooperación efectiva entre las autoridades de control de los diferentes Estados miembros. El buen funcionamiento del mercado interior exige que la libre circulación de los datos personales en la Unión no sea restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales. Con objeto de tener en cuenta la situación específica de las microempresas y las pequeñas y medianas empresas, el presente Reglamento incluye una serie de excepciones en materia de llevanza de registros para organizaciones con menos de 250 empleados. Además, alienta a las instituciones y órganos de la Unión y a los Estados miembros y a sus autoridades de control a tener en cuenta las necesidades específicas de las microempresas y las pequeñas y medianas empresas en la aplicación del presente Reglamento. El concepto de microempresas y pequeñas y medianas empresas debe extraerse del artículo 2 del anexo de la Recomendación 2003/361/CE de la Comisión [(5)].

(14) La protección otorgada por el presente Reglamento debe aplicarse a las personas físicas, independientemente de su nacionalidad o de su lugar de residencia, en relación con el tratamiento de sus datos personales. El presente Reglamento no regula el tratamiento de datos personales relativos a personas jurídicas y en particular a empresas constituidas como personas jurídicas, incluido el nombre y la forma de la persona jurídica y sus datos de contacto.

(15) A fin de evitar que haya un grave riesgo de elusión, la protección de las personas físicas debe ser tecnológicamente neutra y no debe depender de las técnicas utilizadas. La protección de las personas físicas debe aplicarse al tratamiento automatizado de datos personales, así como a su tratamiento manual, cuando los datos personales figuren en un fichero o estén destinados a ser incluidos en él. Los ficheros o conjuntos de ficheros, así como sus portadas, que no estén estructurados con arreglo a criterios específicos, no deben entrar en el ámbito de aplicación del presente Reglamento.

(16) El presente Reglamento no se aplica a cuestiones de protección de los derechos y las libertades fundamentales o la libre circulación de datos personales relacionadas con

actividades excluidas del ámbito de del Derecho de la Unión, como las actividades relativas a la seguridad nacional. Tampoco se aplica al tratamiento de datos de carácter personal por los Estados miembros en el ejercicio de las actividades relacionadas con la política exterior y de seguridad común de la Unión.

(17) El Reglamento (CE) n.º 45/2001 del Parlamento Europeo y del Consejo [(6)] se aplica al tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión. El Reglamento (CE) n.º 45/2001 y otros actos jurídicos de la Unión aplicables a dicho tratamiento de datos de carácter personal deben adaptarse a los principios y normas establecidos en el presente Reglamento y aplicarse a la luz del mismo. A fin de establecer un marco sólido y coherente en materia de protección de datos en la Unión, una vez adoptado el presente Reglamento deben introducirse las adaptaciones necesarias del Reglamento (CE) n.º 45/2001, con el fin de que pueda aplicarse al mismo tiempo que el presente Reglamento.

(18) El presente Reglamento no se aplica al tratamiento de datos de carácter personal por una persona física en el curso de una actividad exclusivamente personal o doméstica y, por tanto, sin conexión alguna con una actividad profesional o comercial. Entre las actividades personales o domésticas cabe incluir la correspondencia y la llevanza de un repertorio de direcciones, o la actividad en las redes sociales y la actividad en línea realizada en el contexto de las citadas actividades. No obstante, el presente Reglamento se aplica a los responsables o encargados del tratamiento que proporcionen los medios para tratar datos personales relacionados con tales actividades personales o domésticas.

(19) La protección de las personas físicas en lo que respecta al tratamiento de datos de carácter personal por parte de las autoridades competentes a efectos de la prevención, investigación, detección o enjuiciamiento de infracciones penales o de la ejecución de sanciones penales, incluida la protección frente a las amenazas contra la seguridad pública y la libre circulación de estos datos y su prevención, es objeto de un acto jurídico específico a nivel de la Unión. El presente Reglamento no debe, por lo tanto, aplicarse a las actividades de tratamiento destinadas a tales fines. No obstante, los datos personales tratados por las autoridades públicas en aplicación del presente Reglamento deben, si se destinan a tales fines, regirse por un acto jurídico de la Unión más específico, concretamente la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo [(7)]. Los Estados miembros pueden encomendar a las autoridades competentes, tal como se definen en la Directiva (UE) 2016/680, funciones que no se lleven a cabo necesariamente con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o ejecución de sanciones penales, incluida la protección frente a las amenazas a la seguridad pública y su prevención, de tal forma que el tratamiento de datos personales para estos otros fines, en la medida en que esté incluido en el ámbito del Derecho de la Unión, entra en el ámbito de aplicación del presente Reglamento.

En lo que respecta al tratamiento de datos personales por parte de dichas autoridades competentes con fines que entren en el ámbito de aplicación del presente Reglamento, los Estados miembros deben tener la posibilidad de mantener o introducir disposiciones más específicas para adaptar la aplicación de las normas del presente Reglamento. Tales disposiciones pueden establecer de forma más precisa requisitos concretos para el tratamiento de datos personales con otros fines por parte de dichas autoridades competentes, tomando en consideración la estructura constitucional, organizativa y administrativa del Estado miembro en cuestión. Cuando el tratamiento de datos personales por organismos privados entre en el ámbito de aplicación del presente Reglamento, este debe disponer que los Estados miembros puedan, en condiciones específicas, limitar conforme a Derecho determinadas obligaciones y derechos siempre que dicha limitación sea una medida necesaria y proporcionada en una sociedad democrática para proteger intereses específicos importantes, entre ellos la seguridad pública y la prevención, la investigación, la detección y el enjuiciamiento de infracciones penales o la ejecución de sanciones penales, inclusive la protección frente a las amenazas contra la seguridad pública y su prevención. Esto se aplica, por ejemplo, en el marco de la lucha contra el blanqueo de capitales o de las actividades de los laboratorios de policía científica.

(20) Aunque el presente Reglamento se aplica, entre otras, a las actividades de los tribunales y otras autoridades judiciales, en virtud del Derecho de la Unión o de los Estados

miembros pueden especificarse las operaciones de tratamiento y los procedimientos de tratamiento en relación con el tratamiento de datos personales por los tribunales y otras autoridades judiciales. A fin de preservar la independencia del poder judicial en el desempeño de sus funciones, incluida la toma de decisiones, la competencia de las autoridades de control no debe abarcar el tratamiento de datos personales cuando los tribunales actúen en ejercicio de su función judicial. El control de esas operaciones de tratamiento de datos ha de poder encomendarse a organismos específicos establecidos dentro del sistema judicial del Estado miembro, los cuales deben, en particular, garantizar el cumplimiento de las normas del presente Reglamento, concienciar más a los miembros del poder judicial acerca de sus obligaciones en virtud de este y atender las reclamaciones en relación con tales operaciones de tratamiento de datos.

(21) El presente Reglamento debe entenderse sin perjuicio de la aplicación de la Directiva 2000/31/CE del Parlamento Europeo y del Consejo [(8)], en particular de las normas en materia de responsabilidad de los prestadores de servicios intermediarios establecidas en sus artículos 12 a 15. El objetivo de dicha Directiva es contribuir al correcto funcionamiento del mercado interior garantizando la libre circulación de los servicios de la sociedad de la información entre los Estados miembros.

(22) Todo tratamiento de datos personales en el contexto de las actividades de un establecimiento de un responsable o un encargado del tratamiento en la Unión debe llevarse a cabo de conformidad con el presente Reglamento, independientemente de que el tratamiento tenga lugar en la Unión. Un establecimiento implica el ejercicio de manera efectiva y real de una actividad a través de modalidades estables. La forma jurídica que revistan tales modalidades, ya sea una sucursal o una filial con personalidad jurídica, no es el factor determinante al respecto.

(23) Con el fin de garantizar que las personas físicas no se vean privadas de la protección a la que tienen derecho en virtud del presente Reglamento, el tratamiento de datos personales de interesados que se encuentran en la Unión por un responsable o un encargado no establecido en la Unión debe regirse por el presente Reglamento si las actividades de tratamiento se refieren a la oferta de bienes o servicios a dichos interesados, independientemente de que medie pago. Para determinar si dicho responsable o encargado ofrece bienes o servicios a interesados que se encuentran en la Unión, debe determinarse si es evidente que el responsable o el encargado proyecta ofrecer servicios a interesados en uno o varios de los Estados miembros de la Unión. Si bien la mera accesibilidad del sitio web del responsable o encargado o de un intermediario en la Unión, de una dirección de correo electrónico u otros datos de contacto, o el uso de una lengua generalmente utilizada en el tercer país donde resida el responsable del tratamiento, no basta para determinar dicha intención, hay factores, como el uso de una lengua o una moneda utilizada generalmente en uno o varios Estados miembros con la posibilidad de encargar bienes y servicios en esa otra lengua, o la mención de clientes o usuarios que residen en la Unión, que pueden revelar que el responsable del tratamiento proyecta ofrecer bienes o servicios a interesados en la Unión.

(24) El tratamiento de datos personales de los interesados que se encuentran en la Unión por un responsable o encargado no establecido en la Unión debe ser también objeto del presente Reglamento cuando esté relacionado con la observación del comportamiento de dichos interesados en la medida en que este comportamiento tenga lugar en la Unión. Para determinar si se puede considerar que una actividad de tratamiento controla el comportamiento de los interesados, debe evaluarse si las personas físicas son objeto de un seguimiento en internet, inclusive el potencial uso posterior de técnicas de tratamiento de datos personales que consistan en la elaboración de un perfil de una persona física con el fin, en particular, de adoptar decisiones sobre él o de analizar o predecir sus preferencias personales, comportamientos y actitudes.

(25) Cuando sea de aplicación el Derecho de los Estados miembros en virtud del Derecho internacional público, el presente Reglamento debe aplicarse también a todo responsable del tratamiento no establecido en la Unión, como en una misión diplomática u oficina consular de un Estado miembro.

(26) Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable. Los datos personales seudonimizados, que cabría atribuir a una persona física mediante la utilización de

información adicional, deben considerarse información sobre una persona física identificable. Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física. Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos. Por lo tanto los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo. En consecuencia, el presente Reglamento no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación.

(27) El presente Reglamento no se aplica a la protección de datos personales de personas fallecidas. Los Estados miembros son competentes para establecer normas relativas al tratamiento de los datos personales de estas.

(28) La aplicación de la seudonimización a los datos personales puede reducir los riesgos para los interesados afectados y ayudar a los responsables y a los encargados del tratamiento a cumplir sus obligaciones de protección de los datos. Así pues, la introducción explícita de la «seudonimización» en el presente Reglamento no pretende excluir ninguna otra medida relativa a la protección de los datos.

(29) Para incentivar la aplicación de la seudonimización en el tratamiento de datos personales, debe ser posible establecer medidas de seudonimización, permitiendo al mismo tiempo un análisis general, por parte del mismo responsable del tratamiento, cuando este haya adoptado las medidas técnicas y organizativas necesarias para garantizar que se aplique el presente Reglamento al tratamiento correspondiente y que se mantenga por separado la información adicional para la atribución de los datos personales a una persona concreta. El responsable que trate datos personales debe indicar cuáles son sus personas autorizadas.

(30) Las personas físicas pueden ser asociadas a identificadores en línea facilitados por sus dispositivos, aplicaciones, herramientas y protocolos, como direcciones de los protocolos de internet, identificadores de sesión en forma de «cookies» u otros identificadores, como etiquetas de identificación por radiofrecuencia. Esto puede dejar huellas que, en particular, al ser combinadas con identificadores únicos y otros datos recibidos por los servidores, pueden ser utilizadas para elaborar perfiles de las personas físicas e identificarlas.

(31) Las autoridades públicas a las que se comunican datos personales en virtud de una obligación legal para el ejercicio de su misión oficial, como las autoridades fiscales y aduaneras, las unidades de investigación financiera, las autoridades administrativas independientes o los organismos de supervisión de los mercados financieros encargados de la reglamentación y supervisión de los mercados de valores, no deben considerarse destinatarios de datos si reciben datos personales que son necesarios para llevar a cabo una investigación concreta de interés general, de conformidad con el Derecho de la Unión o de los Estados miembros. Las solicitudes de comunicación de las autoridades públicas siempre deben presentarse por escrito, de forma motivada y con carácter ocasional, y no deben referirse a la totalidad de un fichero ni dar lugar a la interconexión de varios ficheros. El tratamiento de datos personales por dichas autoridades públicas debe ser conforme con la normativa en materia de protección de datos que sea de aplicación en función de la finalidad del tratamiento.

(32) El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. El consentimiento debe darse para todas las

actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos. Si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta.

(33) Con frecuencia no es posible determinar totalmente la finalidad del tratamiento de los datos personales con fines de investigación científica en el momento de su recogida. Por consiguiente, debe permitirse a los interesados dar su consentimiento para determinados ámbitos de investigación científica que respeten las normas éticas reconocidas para la investigación científica. Los interesados deben tener la oportunidad de dar su consentimiento solamente para determinadas áreas de investigación o partes de proyectos de investigación, en la medida en que lo permita la finalidad perseguida.

(34) Debe entenderse por datos genéticos los datos personales relacionados con características genéticas, heredadas o adquiridas, de una persona física, provenientes del análisis de una muestra biológica de la persona física en cuestión, en particular a través de un análisis cromosómico, un análisis del ácido desoxirribonucleico (ADN) o del ácido ribonucleico (ARN), o del análisis de cualquier otro elemento que permita obtener información equivalente.

(35) Entre los datos personales relativos a la salud se deben incluir todos los datos relativos al estado de salud del interesado que dan información sobre su estado de salud física o mental pasado, presente o futuro. Se incluye la información sobre la persona física recogida con ocasión de su inscripción a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia, de conformidad con la Directiva 2011/24/UE del Parlamento Europeo y del Consejo [(9)]; todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro.

(36) El establecimiento principal de un responsable del tratamiento en la Unión debe ser el lugar de su administración central en la Unión, salvo que las decisiones relativas a los fines y medios del tratamiento de los datos personales se tomen en otro establecimiento del responsable en la Unión, en cuyo caso, ese otro establecimiento debe considerarse el establecimiento principal. El establecimiento principal de un responsable en la Unión debe determinarse en función de criterios objetivos y debe implicar el ejercicio efectivo y real de actividades de gestión que determinen las principales decisiones en cuanto a los fines y medios del tratamiento a través de modalidades estables. Dicho criterio no debe depender de si el tratamiento de los datos personales se realiza en dicho lugar. La presencia y utilización de medios técnicos y tecnologías para el tratamiento de datos personales o las actividades de tratamiento no constituyen, en sí mismas, establecimiento principal y no son, por lo tanto, criterios determinantes de un establecimiento principal. El establecimiento principal del encargado del tratamiento debe ser el lugar de su administración central en la Unión o, si careciese de administración central en la Unión, el lugar en el que se llevan a cabo las principales actividades de tratamiento en la Unión. En los casos que impliquen tanto al responsable como al encargado, la autoridad de control principal competente debe seguir siendo la autoridad de control del Estado miembro en el que el responsable tenga su establecimiento principal, pero la autoridad de control del encargado debe considerarse autoridad de control interesada y participar en el procedimiento de cooperación establecido en el presente Reglamento. En cualquier caso, las autoridades de control del Estado miembro o los Estados miembros en los que el encargado tenga uno o varios establecimientos no deben considerarse autoridades de control interesadas cuando el proyecto de decisión afecte únicamente al responsable. Cuando el tratamiento lo realice un grupo empresarial, el establecimiento principal de la empresa que ejerce el control debe considerarse el establecimiento principal del grupo empresarial, excepto cuando los fines y medios del tratamiento los determine otra empresa.

(37) Un grupo empresarial debe estar constituido por una empresa que ejerce el control y las empresas controladas, debiendo ser la empresa que ejerce el control la que pueda ejercer una influencia dominante en las otras empresas, por razones, por ejemplo, de propiedad, participación financiera, normas por las que se rige, o poder de hacer cumplir las normas de protección de datos personales. Una empresa que controle el tratamiento de los datos personales en las empresas que estén afiliadas debe considerarse, junto con dichas empresas, «grupo empresarial».

(38) Los niños merecen una protección específica de sus datos personales, ya que pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales. Dicha protección específica debe aplicarse en particular, a la utilización de datos personales de niños con fines de mercadotecnia o elaboración de perfiles de personalidad o de usuario, y a la obtención de datos personales relativos a niños cuando se utilicen servicios ofrecidos directamente a un niño. El consentimiento del titular de la patria potestad o tutela no debe ser necesario en el contexto de los servicios preventivos o de asesoramiento ofrecidos directamente a los niños.

(39) Todo tratamiento de datos personales debe ser lícito y leal. Para las personas físicas debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados. El principio de transparencia exige que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro. Dicho principio se refiere en particular a la información de los interesados sobre la identidad del responsable del tratamiento y los fines del mismo y a la información añadida para garantizar un tratamiento leal y transparente con respecto a las personas físicas afectadas y a su derecho a obtener confirmación y comunicación de los datos personales que les conciernan que sean objeto de tratamiento. Las personas físicas deben tener conocimiento de los riesgos, las normas, las salvaguardias y los derechos relativos al tratamiento de datos personales así como del modo de hacer valer sus derechos en relación con el tratamiento. En particular, los fines específicos del tratamiento de los datos personales deben ser explícitos y legítimos, y deben determinarse en el momento de su recogida. Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario para los fines para los que sean tratados. Ello requiere, en particular, garantizar que se limite a un mínimo estricto su plazo de conservación. Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios. Para garantizar que los datos personales no se conservan más tiempo del necesario, el responsable del tratamiento ha de establecer plazos para su supresión o revisión periódica. Deben tomarse todas las medidas razonables para garantizar que se rectifiquen o supriman los datos personales que sean inexactos. Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento.

(40) Para que el tratamiento sea lícito, los datos personales deben ser tratados con el consentimiento del interesado o sobre alguna otra base legítima establecida conforme a Derecho, ya sea en el presente Reglamento o en virtud de otro Derecho de la Unión o de los Estados miembros a que se refiera el presente Reglamento, incluida la necesidad de cumplir la obligación legal aplicable al responsable del tratamiento o la necesidad de ejecutar un contrato en el que sea parte el interesado o con objeto de tomar medidas a instancia del interesado con anterioridad a la conclusión de un contrato.

(41) Cuando el presente Reglamento hace referencia a una base jurídica o a una medida legislativa, esto no exige necesariamente un acto legislativo adoptado por un parlamento, sin perjuicio de los requisitos de conformidad del ordenamiento constitucional del Estado miembro de que se trate. Sin embargo, dicha base jurídica o medida legislativa debe ser clara y precisa y su aplicación previsible para sus destinatarios, de conformidad con la jurisprudencia del Tribunal de Justicia de la Unión Europea (en lo sucesivo, «Tribunal de Justicia») y del Tribunal Europeo de Derechos Humanos.

(42) Cuando el tratamiento se lleva a cabo con el consentimiento del interesado, el responsable del tratamiento debe ser capaz de demostrar que aquel ha dado su consentimiento a la operación de tratamiento. En particular en el contexto de una declaración

por escrito efectuada sobre otro asunto, debe haber garantías de que el interesado es consciente del hecho de que da su consentimiento y de la medida en que lo hace. De acuerdo con la Directiva 93/13/CEE del Consejo [10], debe proporcionarse un modelo de declaración de consentimiento elaborado previamente por el responsable del tratamiento con una formulación inteligible y de fácil acceso que emplee un lenguaje claro y sencillo, y que no contenga cláusulas abusivas. Para que el consentimiento sea informado, el interesado debe conocer como mínimo la identidad del responsable del tratamiento y los fines del tratamiento a los cuales están destinados los datos personales. El consentimiento no debe considerarse libremente prestado cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno.

(43) Para garantizar que el consentimiento se haya dado libremente, este no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibro claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública y sea por lo tanto improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular. Se presume que el consentimiento no se ha dado libremente cuando no permita autorizar por separado las distintas operaciones de tratamiento de datos personales pese a ser adecuado en el caso concreto, o cuando el cumplimiento de un contrato, incluida la prestación de un servicio, sea dependiente del consentimiento, aún cuando este no sea necesario para dicho cumplimiento.

(44) El tratamiento debe ser lícito cuando sea necesario en el contexto de un contrato o de la intención de concluir un contrato.

(45) Cuando se realice en cumplimiento de una obligación legal aplicable al responsable del tratamiento, o si es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos, el tratamiento debe tener una base en el Derecho de la Unión o de los Estados miembros. El presente Reglamento no requiere que cada tratamiento individual se rija por una norma específica. Una norma puede ser suficiente como base para varias operaciones de tratamiento de datos basadas en una obligación legal aplicable al responsable del tratamiento, o si el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos. La finalidad del tratamiento también debe determinase en virtud del Derecho de la Unión o de los Estados miembros. Además, dicha norma podría especificar las condiciones generales del presente Reglamento por las que se rige la licitud del tratamiento de datos personales, establecer especificaciones para la determinación del responsable del tratamiento, el tipo de datos personales objeto de tratamiento, los interesados afectados, las entidades a las que se pueden comunicar los datos personales, las limitaciones de la finalidad, el plazo de conservación de los datos y otras medidas para garantizar un tratamiento lícito y leal. Debe determinarse también en virtud del Derecho de la Unión o de los Estados miembros si el responsable del tratamiento que realiza una misión en interés público o en el ejercicio de poderes públicos debe ser una autoridad pública u otra persona física o jurídica de Derecho público, o, cuando se haga en interés público, incluidos fines sanitarios como la salud pública, la protección social y la gestión de los servicios de sanidad, de Derecho privado, como una asociación profesional.

(46) El tratamiento de datos personales también debe considerarse lícito cuando sea necesario para proteger un interés esencial para la vida del interesado o la de otra persona física. En principio, los datos personales únicamente deben tratarse sobre la base del interés vital de otra persona física cuando el tratamiento no pueda basarse manifiestamente en una base jurídica diferente. Ciertos tipos de tratamiento pueden responder tanto a motivos importantes de interés público como a los intereses vitales del interesado, como por ejemplo cuando el tratamiento es necesario para fines humanitarios, incluido el control de epidemias y su propagación, o en situaciones de emergencia humanitaria, sobre todo en caso de catástrofes naturales o de origen humano.

(47) El interés legítimo de un responsable del tratamiento, incluso el de un responsable al que se puedan comunicar datos personales, o de un tercero, puede constituir una base jurídica para el tratamiento, siempre que no prevalezcan los intereses o los derechos y libertades del interesado, teniendo en cuenta las expectativas razonables de los interesados basadas en su relación con el responsable. Tal interés legítimo podría darse, por ejemplo,

cuando existe una relación pertinente y apropiada entre el interesado y el responsable, como en situaciones en las que el interesado es cliente o está al servicio del responsable. En cualquier caso, la existencia de un interés legítimo requeriría una evaluación meticulosa, inclusive si un interesado puede prever de forma razonable, en el momento y en el contexto de la recogida de datos personales, que pueda producirse el tratamiento con tal fin. En particular, los intereses y los derechos fundamentales del interesado podrían prevalecer sobre los intereses del responsable del tratamiento cuando se proceda al tratamiento de los datos personales en circunstancias en las que el interesado no espere razonablemente que se realice un tratamiento ulterior. Dado que corresponde al legislador establecer por ley la base jurídica para el tratamiento de datos personales por parte de las autoridades públicas, esta base jurídica no debe aplicarse al tratamiento efectuado por las autoridades públicas en el ejercicio de sus funciones. El tratamiento de datos de carácter personal estrictamente necesario para la prevención del fraude constituye también un interés legítimo del responsable del tratamiento de que se trate. El tratamiento de datos personales con fines de mercadotecnia directa puede considerarse realizado por interés legítimo.

(48) Los responsables que forman parte de un grupo empresarial o de entidades afiliadas a un organismo central pueden tener un interés legítimo en transmitir datos personales dentro del grupo empresarial para fines administrativos internos, incluido el tratamiento de datos personales de clientes o empleados. Los principios generales aplicables a la transmisión de datos personales, dentro de un grupo empresarial, a una empresa situada en un país tercero no se ven afectados.

(49) Constituye un interés legítimo del responsable del tratamiento interesado el tratamiento de datos personales en la medida estrictamente necesaria y proporcionada para garantizar la seguridad de la red y de la información, es decir la capacidad de una red o de un sistema información de resistir, en un nivel determinado de confianza, a acontecimientos accidentales o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos personales conservados o transmitidos, y la seguridad de los servicios conexos ofrecidos por, o accesibles a través de, estos sistemas y redes, por parte de autoridades públicas, equipos de respuesta a emergencias informáticas (CERT), equipos de respuesta a incidentes de seguridad informática (CSIRT), proveedores de redes y servicios de comunicaciones electrónicas y proveedores de tecnologías y servicios de seguridad. En lo anterior cabría incluir, por ejemplo, impedir el acceso no autorizado a las redes de comunicaciones electrónicas y la distribución malintencionada de códigos, y frenar ataques de «denegación de servicio» y daños a los sistemas informáticos y de comunicaciones electrónicas.

(50) El tratamiento de datos personales con fines distintos de aquellos para los que hayan sido recogidos inicialmente solo debe permitirse cuando sea compatible con los fines de su recogida inicial. En tal caso, no se requiere una base jurídica aparte, distinta de la que permitió la obtención de los datos personales. Si el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, los cometidos y los fines para los cuales se debe considerar compatible y lícito el tratamiento ulterior se pueden determinar y especificar de acuerdo con el Derecho de la Unión o de los Estados miembros. Las operaciones de tratamiento ulterior con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos deben considerarse operaciones de tratamiento lícitas compatibles. La base jurídica establecida en el Derecho de la Unión o de los Estados miembros para el tratamiento de datos personales también puede servir de base jurídica para el tratamiento ulterior. Con objeto de determinar si el fin del tratamiento ulterior es compatible con el fin de la recogida inicial de los datos personales, el responsable del tratamiento, tras haber cumplido todos los requisitos para la licitud del tratamiento original, debe tener en cuenta, entre otras cosas, cualquier relación entre estos fines y los fines del tratamiento ulterior previsto, el contexto en el que se recogieron los datos, en particular las expectativas razonables del interesado basadas en su relación con el responsable en cuanto a su uso posterior, la naturaleza de los datos personales, las consecuencias para los interesados del tratamiento ulterior previsto y la existencia de garantías adecuadas tanto en la operación de tratamiento original como en la operación de tratamiento ulterior prevista.

Si el interesado dio su consentimiento o el tratamiento se basa en el Derecho de la Unión o de los Estados miembros que constituye una medida necesaria y proporcionada en una sociedad democrática para salvaguardar, en particular, objetivos importantes de interés público general, el responsable debe estar facultado para el tratamiento ulterior de los datos personales, con independencia de la compatibilidad de los fines. En todo caso, se debe garantizar la aplicación de los principios establecidos por el presente Reglamento y, en particular, la información del interesado sobre esos otros fines y sobre sus derechos, incluido el derecho de oposición. La indicación de posibles actos delictivos o amenazas para la seguridad pública por parte del responsable del tratamiento y la transmisión a la autoridad competente de los datos respecto de casos individuales o casos diversos relacionados con un mismo acto delictivo o amenaza para la seguridad pública debe considerarse que es en interés legítimo del responsable. Con todo, debe prohibirse esa transmisión en interés legítimo del responsable o el tratamiento ulterior de datos personales si el tratamiento no es compatible con una obligación de secreto legal, profesional o vinculante por otro concepto.

(51) Especial protección merecen los datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales. Debe incluirse entre tales datos personales los datos de carácter personal que revelen el origen racial o étnico, entendiéndose que el uso del término «origen racial» en el presente Reglamento no implica la aceptación por parte de la Unión de teorías que traten de determinar la existencia de razas humanas separadas. El tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física. Tales datos personales no deben ser tratados, a menos que se permita su tratamiento en situaciones específicas contempladas en el presente Reglamento, habida cuenta de que los Estados miembros pueden establecer disposiciones específicas sobre protección de datos con objeto de adaptar la aplicación de las normas del presente Reglamento al cumplimiento de una obligación legal o al cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Además de los requisitos específicos de ese tratamiento, deben aplicarse los principios generales y otras normas del presente Reglamento, sobre todo en lo que se refiere a las condiciones de licitud del tratamiento. Se deben establecer de forma explícita excepciones a la prohibición general de tratamiento de esas categorías especiales de datos personales, entre otras cosas cuando el interesado dé su consentimiento explícito o tratándose de necesidades específicas, en particular cuando el tratamiento sea realizado en el marco de actividades legítimas por determinadas asociaciones o fundaciones cuyo objetivo sea permitir el ejercicio de las libertades fundamentales.

(52) Asimismo deben autorizarse excepciones a la prohibición de tratar categorías especiales de datos personales cuando lo establezca el Derecho de la Unión o de los Estados miembros y siempre que se den las garantías apropiadas, a fin de proteger datos personales y otros derechos fundamentales, cuando sea en interés público, en particular el tratamiento de datos personales en el ámbito de la legislación laboral, la legislación sobre protección social, incluidas las pensiones y con fines de seguridad, supervisión y alerta sanitaria, la prevención o control de enfermedades transmisibles y otras amenazas graves para la salud. Tal excepción es posible para fines en el ámbito de la salud, incluidas la sanidad pública y la gestión de los servicios de asistencia sanitaria, especialmente con el fin de garantizar la calidad y la rentabilidad de los procedimientos utilizados para resolver las reclamaciones de prestaciones y de servicios en el régimen del seguro de enfermedad, o con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos. Debe autorizarse asimismo a título excepcional el tratamiento de dichos datos personales cuando sea necesario para la formulación, el ejercicio o la defensa de reclamaciones, ya sea por un procedimiento judicial o un procedimiento administrativo o extrajudicial.

(53) Las categorías especiales de datos personales que merecen mayor protección únicamente deben tratarse con fines relacionados con la salud cuando sea necesario para

lograr dichos fines en beneficio de las personas físicas y de la sociedad en su conjunto, en particular en el contexto de la gestión de los servicios y sistemas sanitarios o de protección social, incluido el tratamiento de esos datos por las autoridades gestoras de la sanidad y las autoridades sanitarias nacionales centrales con fines de control de calidad, gestión de la información y supervisión general nacional y local del sistema sanitario o de protección social, y garantía de la continuidad de la asistencia sanitaria o la protección social y la asistencia sanitaria transfronteriza o fines de seguridad, supervisión y alerta sanitaria, o con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, basados en el Derecho de la Unión o del Estado miembro que ha de cumplir un objetivo de interés público, así como para estudios realizados en interés público en el ámbito de la salud pública. Por tanto, el presente Reglamento debe establecer condiciones armonizadas para el tratamiento de categorías especiales de datos personales relativos a la salud, en relación con necesidades específicas, en particular si el tratamiento de esos datos lo realizan, con fines relacionados con la salud, personas sujetas a la obligación legal de secreto profesional. El Derecho de la Unión o de los Estados miembros debe establecer medidas específicas y adecuadas para proteger los derechos fundamentales y los datos personales de las personas físicas. Los Estados miembros deben estar facultados para mantener o introducir otras condiciones, incluidas limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud. No obstante, esto no ha de suponer un obstáculo para la libre circulación de datos personales dentro de la Unión cuando tales condiciones se apliquen al tratamiento transfronterizo de esos datos.

(54) El tratamiento de categorías especiales de datos personales, sin el consentimiento del interesado, puede ser necesario por razones de interés público en el ámbito de la salud pública. Ese tratamiento debe estar sujeto a medidas adecuadas y específicas a fin de proteger los derechos y libertades de las personas físicas. En ese contexto, «salud pública» debe interpretarse en la definición del Reglamento (CE) n.º 1338/2008 del Parlamento Europeo y del Consejo [11], es decir, todos los elementos relacionados con la salud, concretamente el estado de salud, con inclusión de la morbilidad y la discapacidad, los determinantes que influyen en dicho estado de salud, las necesidades de asistencia sanitaria, los recursos asignados a la asistencia sanitaria, la puesta a disposición de asistencia sanitaria y el acceso universal a ella, así como los gastos y la financiación de la asistencia sanitaria, y las causas de mortalidad. Este tratamiento de datos relativos a la salud por razones de interés público no debe dar lugar a que terceros, como empresarios, compañías de seguros o entidades bancarias, traten los datos personales con otros fines.

(55) Se realiza además por razones de interés público el tratamiento de datos personales por las autoridades públicas con el fin de alcanzar los objetivos, establecidos en el Derecho constitucional o en el Derecho internacional público, de asociaciones religiosas reconocidas oficialmente.

(56) Si, en el marco de actividades electorales, el funcionamiento del sistema democrático exige en un Estado miembro que los partidos políticos recopilen datos personales sobre las opiniones políticas de las personas, puede autorizarse el tratamiento de estos datos por razones de interés público, siempre que se ofrezcan garantías adecuadas.

(57) Si los datos personales tratados por un responsable no le permiten identificar a una persona física, el responsable no debe estar obligado a obtener información adicional para identificar al interesado con la única finalidad de cumplir cualquier disposición del presente Reglamento. No obstante, el responsable del tratamiento no debe negarse a recibir información adicional facilitada por el interesado a fin de respaldarle en el ejercicio de sus derechos. La identificación debe incluir la identificación digital de un interesado, por ejemplo mediante un mecanismo de autenticación, como las mismas credenciales, empleadas por el interesado para abrir una sesión en el servicio en línea ofrecido por el responsable.

(58) El principio de transparencia exige que toda información dirigida al público o al interesado sea concisa, fácilmente accesible y fácil de entender, y que se utilice un lenguaje claro y sencillo, y, además, en su caso, se visualice. Esta información podría facilitarse en forma electrónica, por ejemplo, cuando esté dirigida al público, mediante un sitio web. Ello es especialmente pertinente en situaciones en las que la proliferación de agentes y la complejidad tecnológica de la práctica hagan que sea difícil para el interesado saber y comprender si se están recogiendo, por quién y con qué finalidad, datos personales que le

conciernen, como es en el caso de la publicidad en línea. Dado que los niños merecen una protección específica, cualquier información y comunicación cuyo tratamiento les afecte debe facilitarse en un lenguaje claro y sencillo que sea fácil de entender.

(59) Deben arbitrarse fórmulas para facilitar al interesado el ejercicio de sus derechos en virtud del presente Reglamento, incluidos los mecanismos para solicitar y, en su caso, obtener de forma gratuita, en particular, el acceso a los datos personales y su rectificación o supresión, así como el ejercicio del derecho de oposición. El responsable del tratamiento también debe proporcionar medios para que las solicitudes se presenten por medios electrónicos, en particular cuando los datos personales se tratan por medios electrónicos. El responsable del tratamiento debe estar obligado a responder a las solicitudes del interesado sin dilación indebida y a más tardar en el plazo de un mes, y a explicar sus motivos en caso de que no fuera a atenderlas.

(60) Los principios de tratamiento leal y transparente exigen que se informe al interesado de la existencia de la operación de tratamiento y sus fines. El responsable del tratamiento debe facilitar al interesado cuanta información complementaria sea necesaria para garantizar un tratamiento leal y transparente, habida cuenta de las circunstancias y del contexto específicos en que se traten los datos personales. Se debe además informar al interesado de la existencia de la elaboración de perfiles y de las consecuencias de dicha elaboración. Si los datos personales se obtienen de los interesados, también se les debe informar de si están obligados a facilitarlos y de las consecuencias en caso de que no lo hicieran. Dicha información puede transmitirse en combinación con unos iconos normalizados que ofrezcan, de forma fácilmente visible, inteligible y claramente legible, una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presentan en formato electrónico deben ser legibles mecánicamente.

(61) Se debe facilitar a los interesados la información sobre el tratamiento de sus datos personales en el momento en que se obtengan de ellos o, si se obtienen de otra fuente, en un plazo razonable, dependiendo de las circunstancias del caso. Si los datos personales pueden ser comunicados legítimamente a otro destinatario, se debe informar al interesado en el momento en que se comunican al destinatario por primera vez. El responsable del tratamiento que proyecte tratar los datos para un fin que no sea aquel para el que se recogieron debe proporcionar al interesado, antes de dicho tratamiento ulterior, información sobre ese otro fin y otra información necesaria. Cuando el origen de los datos personales no pueda facilitarse al interesado por haberse utilizado varias fuentes, debe facilitarse información general.

(62) Sin embargo, no es necesario imponer la obligación de proporcionar información cuando el interesado ya posea la información, cuando el registro o la comunicación de los datos personales estén expresamente establecidos por ley, o cuando facilitar la información al interesado resulte imposible o exija un esfuerzo desproporcionado. Tal podría ser particularmente el caso cuando el tratamiento se realice con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos. A este respecto, debe tomarse en consideración el número de interesados, la antigüedad de los datos y las garantías adecuadas adoptadas.

(63) Los interesados deben tener derecho a acceder a los datos personales recogidos que le conciernan y a ejercer dicho derecho con facilidad y a intervalos razonables, con el fin de conocer y verificar la licitud del tratamiento. Ello incluye el derecho de los interesados a acceder a datos relativos a la salud, por ejemplo los datos de sus historias clínicas que contengan información como diagnósticos, resultados de exámenes, evaluaciones de facultativos y cualesquiera tratamientos o intervenciones practicadas. Todo interesado debe, por tanto, tener el derecho a conocer y a que se le comuniquen, en particular, los fines para los que se tratan los datos personales, su plazo de tratamiento, sus destinatarios, la lógica implícita en todo tratamiento automático de datos personales y, por lo menos cuando se base en la elaboración de perfiles, las consecuencias de dicho tratamiento. Si es posible, el responsable del tratamiento debe estar facultado para facilitar acceso remoto a un sistema seguro que ofrezca al interesado un acceso directo a sus datos personales. Este derecho no debe afectar negativamente a los derechos y libertades de terceros, incluidos los secretos comerciales o la propiedad intelectual y, en particular, los derechos de propiedad intelectual que protegen programas informáticos. No obstante, estas consideraciones no deben tener

como resultado la negativa a prestar toda la información al interesado. Si trata una gran cantidad de información relativa al interesado, el responsable del tratamiento debe estar facultado para solicitar que, antes de facilitarse la información, el interesado especifique la información o actividades de tratamiento a que se refiere la solicitud.

(64) El responsable del tratamiento debe utilizar todas las medidas razonables para verificar la identidad de los interesados que soliciten acceso, en particular en el contexto de los servicios en línea y los identificadores en línea. El responsable no debe conservar datos personales con el único propósito de poder responder a posibles solicitudes.

(65) Los interesados deben tener derecho a que se rectifiquen los datos personales que le conciernen y un «derecho al olvido» si la retención de tales datos infringe el presente Reglamento o el Derecho de la Unión o de los Estados miembros aplicable al responsable del tratamiento. En particular, los interesados deben tener derecho a que sus datos personales se supriman y dejen de tratarse si ya no son necesarios para los fines para los que fueron recogidos o tratados de otro modo, si los interesados han retirado su consentimiento para el tratamiento o se oponen al tratamiento de datos personales que les conciernen, o si el tratamiento de sus datos personales incumple de otro modo el presente Reglamento. Este derecho es pertinente en particular si el interesado dio su consentimiento siendo niño y no se es plenamente consciente de los riesgos que implica el tratamiento, y más tarde quiere suprimir tales datos personales, especialmente en internet. El interesado debe poder ejercer este derecho aunque ya no sea un niño. Sin embargo, la retención ulterior de los datos personales debe ser lícita cuando sea necesaria para el ejercicio de la libertad de expresión e información, para el cumplimiento de una obligación legal, para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, por razones de interés público en el ámbito de la salud pública, con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, o para la formulación, el ejercicio o la defensa de reclamaciones.

(66) A fin de reforzar el «derecho al olvido» en el entorno en línea, el derecho de supresión debe ampliarse de tal forma que el responsable del tratamiento que haya hecho públicos datos personales esté obligado a indicar a los responsables del tratamiento que estén tratando tales datos personales que supriman todo enlace a ellos, o las copias o réplicas de tales datos. Al proceder así, dicho responsable debe tomar medidas razonables, teniendo en cuenta la tecnología y los medios a su disposición, incluidas las medidas técnicas, para informar de la solicitud del interesado a los responsables que estén tratando los datos personales.

(67) Entre los métodos para limitar el tratamiento de datos personales cabría incluir los consistentes en trasladar temporalmente los datos seleccionados a otro sistema de tratamiento, en impedir el acceso de usuarios a los datos personales seleccionados o en retirar temporalmente los datos publicados de un sitio internet. En los ficheros automatizados la limitación del tratamiento debe realizarse, en principio, por medios técnicos, de forma que los datos personales no sean objeto de operaciones de tratamiento ulterior ni puedan modificarse. El hecho de que el tratamiento de los datos personales esté limitado debe indicarse claramente en el sistema.

(68) Para reforzar aún más el control sobre sus propios datos, cuando el tratamiento de los datos personales se efectúe por medios automatizados, debe permitirse asimismo que los interesados que hubieran facilitado datos personales que les conciernan a un responsable del tratamiento los reciban en un formato estructurado, de uso común, de lectura mecánica e interoperable, y los transmitan a otro responsable del tratamiento. Debe alentarse a los responsables a crear formatos interoperables que permitan la portabilidad de datos. Dicho derecho debe aplicarse cuando el interesado haya facilitado los datos personales dando su consentimiento o cuando el tratamiento sea necesario para la ejecución de un contrato. No debe aplicarse cuando el tratamiento tiene una base jurídica distinta del consentimiento o el contrato. Por su propia naturaleza, dicho derecho no debe ejercerse en contra de responsables que traten datos personales en el ejercicio de sus funciones públicas. Por lo tanto, no debe aplicarse, cuando el tratamiento de los datos personales sea necesario para cumplir una obligación legal aplicable al responsable o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al

responsable. El derecho del interesado a transmitir o recibir datos personales que lo conciernan no debe obligar al responsable a adoptar o mantener sistemas de tratamiento que sean técnicamente compatibles. Cuando un conjunto de datos personales determinado concierna a más de un interesado, el derecho a recibir tales datos se debe entender sin menoscabo de los derechos y libertades de otros interesados de conformidad con el presente Reglamento. Por otra parte, ese derecho no debe menoscabar el derecho del interesado a obtener la supresión de los datos personales y las limitaciones de ese derecho recogidas en el presente Reglamento, y en particular no debe implicar la supresión de los datos personales concernientes al interesado que este haya facilitado para la ejecución de un contrato, en la medida y durante el tiempo en que los datos personales sean necesarios para la ejecución de dicho contrato. El interesado debe tener derecho a que los datos personales se transmitan directamente de un responsable del tratamiento a otro, cuando sea técnicamente posible.

(69) En los casos en que los datos personales puedan ser tratados lícitamente porque el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento o por motivos de intereses legítimos del responsable o de un tercero, el interesado debe, sin embargo, tener derecho a oponerse al tratamiento de cualquier dato personal relativo a su situación particular. Debe ser el responsable el que demuestre que sus intereses legítimos imperiosos prevalecen sobre los intereses o los derechos y libertades fundamentales del interesado.

(70) Si los datos personales son tratados con fines de mercadotecnia directa, el interesado debe tener derecho a oponerse a dicho tratamiento, inclusive a la elaboración de perfiles en la medida en que esté relacionada con dicha mercadotecnia directa, ya sea con respecto a un tratamiento inicial o ulterior, y ello en cualquier momento y sin coste alguno. Dicho derecho debe comunicarse explícitamente al interesado y presentarse claramente y al margen de cualquier otra información.

(71) El interesado debe tener derecho a no ser objeto de una decisión, que puede incluir una medida, que evalúe aspectos personales relativos a él, y que se base únicamente en el tratamiento automatizado y produzca efectos jurídicos en él o le afecte significativamente de modo similar, como la denegación automática de una solicitud de crédito en línea o los servicios de contratación en red en los que no medie intervención humana alguna. Este tipo de tratamiento incluye la elaboración de perfiles consistente en cualquier forma de tratamiento automatizado de los datos personales que evalúe aspectos personales relativos a una persona física, en particular para analizar o predecir aspectos relacionados con el rendimiento en el trabajo, la situación económica, la salud, las preferencias o intereses personales, la fiabilidad o el comportamiento, la situación o los movimientos del interesado, en la medida en que produzca efectos jurídicos en él o le afecte significativamente de modo similar. Sin embargo, se deben permitir las decisiones basadas en tal tratamiento, incluida la elaboración de perfiles, si lo autoriza expresamente el Derecho de la Unión o de los Estados miembros aplicable al responsable del tratamiento, incluso con fines de control y prevención del fraude y la evasión fiscal, realizada de conformidad con las reglamentaciones, normas y recomendaciones de las instituciones de la Unión o de los órganos de supervisión nacionales y para garantizar la seguridad y la fiabilidad de un servicio prestado por el responsable del tratamiento, o necesario para la conclusión o ejecución de un contrato entre el interesado y un responsable del tratamiento, o en los casos en los que el interesado haya dado su consentimiento explícito. En cualquier caso, dicho tratamiento debe estar sujeto a las garantías apropiadas, entre las que se deben incluir la información específica al interesado y el derecho a obtener intervención humana, a expresar su punto de vista, a recibir una explicación de la decisión tomada después de tal evaluación y a impugnar la decisión. Tal medida no debe afectar a un menor.

A fin de garantizar un tratamiento leal y transparente respecto del interesado, teniendo en cuenta las circunstancias y contexto específicos en los que se tratan los datos personales, el responsable del tratamiento debe utilizar procedimientos matemáticos o estadísticos adecuados para la elaboración de perfiles, aplicar medidas técnicas y organizativas apropiadas para garantizar, en particular, que se corrigen los factores que introducen inexactitudes en los datos personales y se reduce al máximo el riesgo de error, asegurar los datos personales de forma que se tengan en cuenta los posibles riesgos para

los intereses y derechos del interesado e impedir, entre otras cosas, efectos discriminatorios en las personas físicas por motivos de raza u origen étnico, opiniones políticas, religión o creencias, afiliación sindical, condición genética o estado de salud u orientación sexual, o tratamiento que dé lugar a medidas que produzcan tal efecto. Las decisiones automatizadas y la elaboración de perfiles sobre la base de categorías particulares de datos personales únicamente deben permitirse en condiciones específicas.

(72) La elaboración de perfiles está sujeta a las normas del presente Reglamento que rigen el tratamiento de datos personales, como los fundamentos jurídicos del tratamiento o los principios de la protección de datos. El Comité Europeo de Protección de Datos establecido por el presente Reglamento (en lo sucesivo, el «Comité») debe tener la posibilidad de formular orientaciones en este contexto.

(73) El Derecho de la Unión o de los Estados miembros puede imponer restricciones a determinados principios y a los derechos de información, acceso, rectificación o supresión de datos personales, al derecho a la portabilidad de los datos, al derecho de oposición, a las decisiones basadas en la elaboración de perfiles, así como a la comunicación de una violación de la seguridad de los datos personales a un interesado y a determinadas obligaciones conexas de los responsables del tratamiento, en la medida en que sea necesario y proporcionado en una sociedad democrática para salvaguardar la seguridad pública, incluida la protección de la vida humana, especialmente en respuesta a catástrofes naturales o de origen humano, la prevención, investigación y el enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a las amenazas contra la seguridad pública o de violaciones de normas deontológicas en las profesiones reguladas, y su prevención, otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un importante interés económico o financiero de la Unión o de un Estado miembro, la llevanza de registros públicos por razones de interés público general, el tratamiento ulterior de datos personales archivados para ofrecer información específica relacionada con el comportamiento político durante los regímenes de antiguos Estados totalitarios, o la protección del interesado o de los derechos y libertades de otros, incluida la protección social, la salud pública y los fines humanitarios. Dichas restricciones deben ajustarse a lo dispuesto en la Carta y en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales.

(74) Debe quedar establecida la responsabilidad del responsable del tratamiento por cualquier tratamiento de datos personales realizado por él mismo o por su cuenta. En particular, el responsable debe estar obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el presente Reglamento, incluida la eficacia de las medidas. Dichas medidas deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como el riesgo para los derechos y libertades de las personas físicas.

(75) Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados.

(76) La probabilidad y la gravedad del riesgo para los derechos y libertades del interesado debe determinarse con referencia a la naturaleza, el alcance, el contexto y los fines del tratamiento de datos. El riesgo debe ponderarse sobre la base de una evaluación objetiva mediante la cual se determine si las operaciones de tratamiento de datos suponen un riesgo o si el riesgo es alto.

(77) Se podrían proporcionar directrices para la aplicación de medidas oportunas y para demostrar el cumplimiento por parte del responsable o del encargado del tratamiento, especialmente con respecto a la identificación del riesgo relacionado con el tratamiento, a su evaluación en términos de origen, naturaleza, probabilidad y gravedad y a la identificación de buenas prácticas para mitigar el riesgo, que revistan, en particular, la forma de códigos de conducta aprobados, certificaciones aprobadas, directrices dadas por el Comité o indicaciones proporcionadas por un delegado de protección de datos. El Comité también puede emitir directrices sobre operaciones de tratamiento que se considere improbable supongan un alto riesgo para los derechos y libertades de las personas físicas, e indicar qué medidas pueden ser suficientes en dichos casos para afrontar el riesgo en cuestión.

(78) La protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos del presente Reglamento. A fin de poder demostrar la conformidad con el presente Reglamento, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto. Dichas medidas podrían consistir, entre otras, en reducir al máximo el tratamiento de datos personales, seudonimizar lo antes posible los datos personales, dar transparencia a las funciones y el tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad. Al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función, ha de alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones, y que se aseguren, con la debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos. Los principios de la protección de datos desde el diseño y por defecto también deben tenerse en cuenta en el contexto de los contratos públicos.

(79) La protección de los derechos y libertades de los interesados, así como la responsabilidad de los responsables y encargados del tratamiento, también en lo que respecta a la supervisión por parte de las autoridades de control y a las medidas adoptadas por ellas, requieren una atribución clara de las responsabilidades en virtud del presente Reglamento, incluidos los casos en los que un responsable determine los fines y medios del tratamiento de forma conjunta con otros responsables, o en los que el tratamiento se lleve a cabo por cuenta de un responsable.

(80) El responsable o el encargado del tratamiento no establecido en la Unión que esté tratando datos personales de interesados que se encuentran en la Unión y cuyas actividades de tratamiento están relacionadas con la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si se requiere un pago por parte de estos, o con el control de su comportamiento en la medida en que este tenga lugar en la Unión, debe designar a un representante, a menos que el tratamiento sea ocasional, no incluya el tratamiento a gran escala de categorías especiales de datos personales o el tratamiento de datos personales relativos a condenas e infracciones penales, y sea improbable que entrañe un riesgo para los derechos y libertades de las personas físicas, vista la naturaleza, el contexto, el ámbito y los fines del tratamiento, o si el responsable del tratamiento es una autoridad u organismo público. El representante debe actuar por cuenta del responsable o el encargado y puede ser contactado por cualquier autoridad de control. El representante debe ser designado expresamente por mandato escrito del responsable o del encargado para que actúe en su nombre con respecto a las obligaciones que les incumben en virtud del presente Reglamento. La designación de dicho representante no afecta a la responsabilidad del responsable o del encargado en virtud del presente Reglamento. Dicho representante debe

desempeñar sus funciones conforme al mandato recibido del responsable o del encargado, incluida la cooperación con las autoridades de control competentes en relación con cualquier medida que se tome para garantizar el cumplimiento del presente Reglamento. El representante designado debe estar sujeto a medidas coercitivas en caso de incumplimiento por parte del responsable o del encargado.

(81) Para garantizar el cumplimiento de las disposiciones del presente Reglamento respecto del tratamiento que lleve a cabo el encargado por cuenta del responsable, este, al encomendar actividades de tratamiento a un encargado, debe recurrir únicamente a encargados que ofrezcan suficientes garantías, en particular en lo que respecta a conocimientos especializados, fiabilidad y recursos, de cara a la aplicación de medidas técnicas y organizativas que cumplan los requisitos del presente Reglamento, incluida la seguridad del tratamiento. La adhesión del encargado a un código de conducta aprobado o a un mecanismo de certificación aprobado puede servir de elemento para demostrar el cumplimiento de las obligaciones por parte del responsable. El tratamiento por un encargado debe regirse por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros que vincule al encargado con el responsable, que fije el objeto y la duración del tratamiento, la naturaleza y fines del tratamiento, el tipo de datos personales y las categorías de interesados, habida cuenta de las funciones y responsabilidades específicas del encargado en el contexto del tratamiento que ha de llevarse a cabo y del riesgo para los derechos y libertades del interesado. El responsable y el encargado pueden optar por basarse en un contrato individual o en cláusulas contractuales tipo que adopte directamente la Comisión o que primero adopte una autoridad de control de conformidad con el mecanismo de coherencia y posteriormente la Comisión. Una vez finalizado el tratamiento por cuenta del responsable, el encargado debe, a elección de aquel, devolver o suprimir los datos personales, salvo que el Derecho de la Unión o de los Estados miembros aplicable al encargado del tratamiento obligue a conservar los datos.

(82) Para demostrar la conformidad con el presente Reglamento, el responsable o el encargado del tratamiento debe mantener registros de las actividades de tratamiento bajo su responsabilidad. Todos los responsables y encargados están obligados a cooperar con la autoridad de control y a poner a su disposición, previa solicitud, dichos registros, de modo que puedan servir para supervisar las operaciones de tratamiento.

(83) A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales.

(84) A fin de mejorar el cumplimiento del presente Reglamento en aquellos casos en los que sea probable que las operaciones de tratamiento entrañen un alto riesgo para los derechos y libertades de las personas físicas, debe incumbir al responsable del tratamiento la realización de una evaluación de impacto relativa a la protección de datos, que evalúe, en particular, el origen, la naturaleza, la particularidad y la gravedad de dicho riesgo. El resultado de la evaluación debe tenerse en cuenta cuando se decidan las medidas adecuadas que deban tomarse con el fin de demostrar que el tratamiento de los datos personales es conforme con el presente Reglamento. Si una evaluación de impacto relativa a la protección de datos muestra que las operaciones de tratamiento entrañan un alto riesgo que el responsable no puede mitigar con medidas adecuadas en términos de tecnología disponible y costes de aplicación, debe consultarse a la autoridad de control antes del tratamiento.

(85) Si no se toman a tiempo medidas adecuadas, las violaciones de la seguridad de los datos personales pueden entrañar daños y perjuicios físicos, materiales o inmateriales para las personas físicas, como pérdida de control sobre sus datos personales o restricción de

sus derechos, discriminación, usurpación de identidad, pérdidas financieras, reversión no autorizada de la seudonimización, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, o cualquier otro perjuicio económico o social significativo para la persona física en cuestión. Por consiguiente, tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales, el responsable debe, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, notificar la violación de la seguridad de los datos personales a la autoridad de control competente, a menos que el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas. Si dicha notificación no es posible en el plazo de 72 horas, debe acompañarse de una indicación de los motivos de la dilación, pudiendo facilitarse información por fases sin más dilación indebida.

(86) El responsable del tratamiento debe comunicar al interesado sin dilación indebida la violación de la seguridad de los datos personales en caso de que puede entrañar un alto riesgo para sus derechos y libertades, y permitirle tomar las precauciones necesarias. La comunicación debe describir la naturaleza de la violación de la seguridad de los datos personales y las recomendaciones para que la persona física afectada mitigue los potenciales efectos adversos resultantes de la violación. Dichas comunicaciones a los interesados deben realizarse tan pronto como sea razonablemente posible y en estrecha cooperación con la autoridad de control, siguiendo sus orientaciones o las de otras autoridades competentes, como las autoridades policiales. Así, por ejemplo, la necesidad de mitigar un riesgo de daños y perjuicios inmediatos justificaría una rápida comunicación con los interesados, mientras que cabe justificar que la comunicación lleve más tiempo por la necesidad de aplicar medidas adecuadas para impedir violaciones de la seguridad de los datos personales continuas o similares.

(87) Debe verificarse si se ha aplicado toda la protección tecnológica adecuada y se han tomado las medidas organizativas oportunas para determinar de inmediato si se ha producido una violación de la seguridad de los datos personales y para informar sin dilación a la autoridad de control y al interesado. Debe verificarse que la notificación se ha realizado sin dilación indebida teniendo en cuenta, en particular, la naturaleza y gravedad de la violación de la seguridad de los datos personales y sus consecuencias y efectos adversos para el interesado. Dicha notificación puede resultar en una intervención de la autoridad de control de conformidad con las funciones y poderes que establece el presente Reglamento.

(88) Al establecer disposiciones de aplicación sobre el formato y los procedimientos aplicables a la notificación de las violaciones de la seguridad de los datos personales, hay que tener debidamente en cuenta las circunstancias de tal violación, inclusive si los datos personales habían sido protegidos mediante las medidas técnicas de protección adecuadas, limitando eficazmente la probabilidad de usurpación de identidad u otras formas de uso indebido. Asimismo, estas normas y procedimientos deben tener en cuenta los intereses legítimos de las autoridades policiales en caso de que una comunicación prematura pueda obstaculizar innecesariamente la investigación de las circunstancias de una violación de la seguridad de los datos personales.

(89) La Directiva 95/46/CE estableció la obligación general de notificar el tratamiento de datos personales a las autoridades de control. Pese a implicar cargas administrativas y financieras, dicha obligación, sin embargo, no contribuyó en todos los casos a mejorar la protección de los datos personales. Por tanto, estas obligaciones generales de notificación indiscriminada deben eliminarse y sustituirse por procedimientos y mecanismos eficaces que se centren, en su lugar, en los tipos de operaciones de tratamiento que, por su naturaleza, alcance, contexto y fines, entrañen probablemente un alto riesgo para los derechos y libertades de las personas físicas. Estos tipos de operaciones de tratamiento pueden ser, en particular, las que implican el uso de nuevas tecnologías, o son de una nueva clase y el responsable del tratamiento no ha realizado previamente una evaluación de impacto relativa a la protección de datos, o si resultan necesarias visto el tiempo transcurrido desde el tratamiento inicial.

(90) En tales casos, el responsable debe llevar a cabo, antes del tratamiento, una evaluación de impacto relativa a la protección de datos con el fin de valorar la particular

gravedad y probabilidad del alto riesgo, teniendo en cuenta la naturaleza, ámbito, contexto y fines del tratamiento y los orígenes del riesgo. Dicha evaluación de impacto debe incluir, en particular, las medidas, garantías y mecanismos previstos para mitigar el riesgo, garantizar la protección de los datos personales y demostrar la conformidad con el presente Reglamento.

(91) Lo anterior debe aplicarse, en particular, a las operaciones de tratamiento a gran escala que persiguen tratar una cantidad considerable de datos personales a nivel regional, nacional o supranacional y que podrían afectar a un gran número de interesados y entrañen probablemente un alto riesgo, por ejemplo, debido a su sensibilidad, cuando, en función del nivel de conocimientos técnicos alcanzado, se haya utilizado una nueva tecnología a gran escala y a otras operaciones de tratamiento que entrañan un alto riesgo para los derechos y libertades de los interesados, en particular cuando estas operaciones hace más difícil para los interesados el ejercicio de sus derechos. La evaluación de impacto relativa a la protección de datos debe realizarse también en los casos en los que se tratan datos personales para adoptar decisiones relativas a personas físicas concretas a raíz de una evaluación sistemática y exhaustiva de aspectos personales propios de personas físicas, basada en la elaboración de perfiles de dichos datos o a raíz del tratamiento de categorías especiales de datos personales, datos biométricos o datos sobre condenas e infracciones penales o medidas de seguridad conexas. También es necesaria una evaluación de impacto relativa a la protección de datos para el control de zonas de acceso público a gran escala, en particular cuando se utilicen dispositivos optoelectrónicos o para cualquier otro tipo de operación cuando la autoridad de control competente considere que el tratamiento entrañe probablemente un alto riesgo para los derechos y libertades de los interesados, en particular porque impida a los interesados ejercer un derecho o utilizar un servicio o ejecutar un contrato, o porque se efectúe sistemáticamente a gran escala. El tratamiento de datos personales no debe considerarse a gran escala si lo realiza, respecto de datos personales de pacientes o clientes, un solo médico, otro profesional de la salud o abogado. En estos casos, la evaluación de impacto de la protección de datos no debe ser obligatoria.

(92) Hay circunstancias en las que puede ser razonable y económico que una evaluación de impacto relativa a la protección de datos abarque más de un único proyecto, por ejemplo, en el caso de que las autoridades u organismos públicos prevean crear una aplicación o plataforma común de tratamiento, o si varios responsables proyecten introducir una aplicación o un entorno de tratamiento común en un sector o segmento empresarial o para una actividad horizontal de uso generalizado.

(93) Los Estados miembros, al adoptar el Derecho en el que se basa el desempeño de las funciones de la autoridad pública o el organismo público y que regula la operación o el conjunto de operaciones de tratamiento en cuestión, pueden considerar necesario llevar a cabo dicha evaluación con carácter previo a las actividades de tratamiento.

(94) Debe consultarse a la autoridad de control antes de iniciar las actividades de tratamiento si una evaluación de impacto relativa a la protección de datos muestra que, en ausencia de garantías, medidas de seguridad y mecanismos destinados a mitigar los riesgos, el tratamiento entrañaría un alto riesgo para los derechos y libertades de las personas físicas, y el responsable del tratamiento considera que el riesgo no puede mitigarse por medios razonables en cuanto a tecnología disponible y costes de aplicación. Existe la probabilidad de que ese alto riesgo se deba a determinados tipos de tratamiento y al alcance y frecuencia de este, lo que también puede ocasionar daños y perjuicios o una injerencia en los derechos y libertades de la persona física. La autoridad de control debe responder a la solicitud de consulta dentro de un plazo determinado. Sin embargo, la ausencia de respuesta de la autoridad de control dentro de dicho plazo no debe obstar a cualquier intervención de dicha autoridad basada en las funciones y poderes que le atribuye el presente Reglamento, incluido el poder de prohibir operaciones de tratamiento. Como parte de dicho proceso de consulta, se puede presentar a la autoridad de control el resultado de una evaluación de impacto relativa a la protección de datos efectuada en relación con el tratamiento en cuestión, en particular las medidas previstas para mitigar los riesgos para los derechos y libertades de las personas físicas.

(95) El encargado del tratamiento debe asistir al responsable cuando sea necesario y a petición suya, a fin de asegurar que se cumplen las obligaciones que se derivan de la

realización de las evaluaciones de impacto relativas a la protección de datos y de la consulta previa a la autoridad de control.

(96) Deben llevarse también a cabo consultas con la autoridad de control en el curso de la tramitación de una medida legislativa o reglamentaria que establezca el tratamiento de datos personales, a fin de garantizar la conformidad del tratamiento previsto con el presente Reglamento y, en particular, de mitigar el riesgo que implique el tratamiento para el interesado.

(97) Al supervisar la observancia interna del presente Reglamento, el responsable o el encargado del tratamiento debe contar con la ayuda de una persona con conocimientos especializados del Derecho y la práctica en materia de protección de datos si el tratamiento lo realiza una autoridad pública, a excepción de los tribunales u otras autoridades judiciales independientes en el ejercicio de su función judicial, si el tratamiento lo realiza en el sector privado un responsable cuyas actividades principales consisten en operaciones de tratamiento a gran escala que requieren un seguimiento habitual y sistemático de los interesados, o si las actividades principales del responsable o del encargado consisten en el tratamiento a gran escala de categorías especiales de datos personales y de datos relativos a condenas e infracciones penales. En el sector privado, las actividades principales de un responsable están relacionadas con sus actividades primarias y no están relacionadas con el tratamiento de datos personales como actividades auxiliares. El nivel de conocimientos especializados necesario se debe determinar, en particular, en función de las operaciones de tratamiento de datos que se lleven a cabo y de la protección exigida para los datos personales tratados por el responsable o el encargado. Tales delegados de protección de datos, sean o no empleados del responsable del tratamiento, deben estar en condiciones de desempeñar sus funciones y cometidos de manera independiente.

(98) Se debe incitar a las asociaciones u otros organismos que representen a categorías de responsables o encargados a que elaboren códigos de conducta, dentro de los límites fijados por el presente Reglamento, con el fin de facilitar su aplicación efectiva, teniendo en cuenta las características específicas del tratamiento llevado a cabo en determinados sectores y las necesidades específicas de las microempresas y las pequeñas y medianas empresas. Dichos códigos de conducta podrían en particular establecer las obligaciones de los responsables y encargados, teniendo en cuenta el riesgo probable para los derechos y libertades de las personas físicas que se derive del tratamiento.

(99) Al elaborar un código de conducta, o al modificar o ampliar dicho código, las asociaciones y otros organismos que representan a categorías de responsables o encargados deben consultar a las partes interesadas, incluidos los interesados cuando sea posible, y tener en cuenta las consideraciones transmitidas y las opiniones manifestadas en respuesta a dichas consultas.

(100) A fin de aumentar la transparencia y el cumplimiento del presente Reglamento, debe fomentarse el establecimiento de mecanismos de certificación y sellos y marcas de protección de datos, que permitan a los interesados evaluar con mayor rapidez el nivel de protección de datos de los productos y servicios correspondientes.

(101) Los flujos transfronterizos de datos personales a, y desde, países no pertenecientes a la Unión y organizaciones internacionales son necesarios para la expansión del comercio y la cooperación internacionales. El aumento de estos flujos plantea nuevos retos e inquietudes en lo que respecta a la protección de los datos de carácter personal. No obstante, si los datos personales se transfieren de la Unión a responsables, encargados u otros destinatarios en terceros países o a organizaciones internacionales, esto no debe menoscabar el nivel de protección de las personas físicas garantizado en la Unión por el presente Reglamento, ni siquiera en las transferencias ulteriores de datos personales desde el tercer país u organización internacional a responsables y encargados en el mismo u otro tercer país u organización internacional. En todo caso, las transferencias a terceros países y organizaciones internacionales solo pueden llevarse a cabo de plena conformidad con el presente Reglamento. Una transferencia solo podría tener lugar si, a reserva de las demás disposiciones del presente Reglamento, el responsable o encargado cumple las disposiciones del presente Reglamento relativas a la transferencia de datos personales a terceros países u organizaciones internacionales.

(102) El presente Reglamento se entiende sin perjuicio de los acuerdos internacionales celebrados entre la Unión y terceros países que regulan la transferencia de datos personales, incluidas las oportunas garantías para los interesados. Los Estados miembros pueden celebrar acuerdos internacionales que impliquen la transferencia de datos personales a terceros países u organizaciones internacionales siempre que dichos acuerdos no afecten al presente Reglamento ni a ninguna otra disposición del Derecho de la Unión e incluyan un nivel adecuado de protección de los derechos fundamentales de los interesados.

(103) La Comisión puede decidir, con efectos para toda la Unión, que un tercer país, un territorio o un sector específico de un tercer país, o una organización internacional ofrece un nivel de protección de datos adecuado, aportando de esta forma en toda la Unión seguridad y uniformidad jurídicas en lo que se refiere al tercer país u organización internacional que se considera ofrece tal nivel de protección. En estos casos, se pueden realizar transferencias de datos personales a estos países sin que se requiera obtener otro tipo de autorización. La Comisión también puede decidir revocar esa decisión, previo aviso y completa declaración motivada al tercer país u organización internacional.

(104) En consonancia con los valores fundamentales en los que se basa la Unión, en particular la protección de los derechos humanos, la Comisión, en su evaluación del tercer país, o de un territorio o un sector específico de un tercer país, debe tener en cuenta de qué manera respeta un determinado tercer país respeta el Estado de Derecho, el acceso a la justicia y las normas y criterios internacionales en materia de derechos humanos y su Derecho general y sectorial, incluida la legislación relativa a la seguridad pública, la defensa y la seguridad nacional, así como el orden público y el Derecho penal. En la adopción de una decisión de adecuación con respecto a un territorio o un sector específico de un tercer país se deben tener en cuenta criterios claros y objetivos, como las actividades concretas de tratamiento y el alcance de las normas jurídicas aplicables y la legislación vigente en el tercer país. El tercer país debe ofrecer garantías que aseguren un nivel adecuado de protección equivalente en lo esencial al ofrecido en la Unión, en particular cuando los datos personales son objeto de tratamiento en uno o varios sectores específicos. En particular, el tercer país debe garantizar que haya un control verdaderamente independiente de la protección de datos y establecer mecanismos de cooperación con las autoridades de protección de datos de los Estados miembros, así como reconocer a los interesados derechos efectivos y exigibles y acciones administrativas y judiciales efectivas.

(105) Aparte de los compromisos internacionales adquiridos por el tercer país u organización internacional, la Comisión debe tener en cuenta las obligaciones resultantes de la participación del tercer país u organización internacional en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales, y el cumplimiento de esas obligaciones. En particular, debe tenerse en cuenta la adhesión del país al Convenio del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y su Protocolo adicional. La Comisión debe consultar al Comité al evaluar el nivel de protección existente en terceros países u organizaciones internacionales.

(106) La Comisión debe supervisar la aplicación de las decisiones sobre el nivel de protección en un país tercero, un territorio o un sector específico de un país tercero, o una organización internacional, y la aplicación las decisiones adoptadas sobre la base del artículo 25, apartado 6, o el artículo 26, apartado 4, de la Directiva 95/46/CE. En sus decisiones de adecuación, la Comisión debe establecer un mecanismo para la revisión periódica de su aplicación. Dicha revisión periódica debe realizarse en colaboración con el tercer país u organización internacional de que se trate y tener en cuenta todos los cambios en la materia que se produzcan en dicho tercer país u organización internacional. A efectos de la supervisión y realización de las revisiones periódicas, la Comisión debe tomar en consideración las opiniones y conclusiones del Parlamento Europeo y del Consejo, así como de otros organismos y fuentes pertinentes. La Comisión debe evaluar, en un plazo razonable, la aplicación de dichas decisiones e informar de cualquier conclusión pertinente al Comité que, en el sentido del Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo [(12)], establece el presente Reglamento, y al Parlamento Europeo y el Consejo.

(107) La Comisión puede reconocer que un tercer país, un territorio o sector específico en un tercer país, o una organización internacional ya no garantiza un nivel de protección de

datos adecuado. En consecuencia, debe prohibirse la transferencia de datos personales a dicho tercer país u organización internacional, salvo que se cumplan los requisitos del presente Reglamento relativos a las transferencias basadas en garantías adecuadas, incluidas las normas corporativas vinculantes, y a las excepciones aplicadas a situaciones específicas. En ese caso, debe establecerse la celebración de consultas entre la Comisión y esos terceros países u organizaciones internacionales. La Comisión debe informar en tiempo oportuno al tercer país u organización internacional de las razones y entablar consultas a fin de subsanar la situación.

(108) En ausencia de una decisión por la que se constate la adecuación de la protección de los datos, el responsable o el encargado del tratamiento deben tomar medidas para compensar la falta de protección de datos en un tercer país mediante garantías adecuadas para el interesado. Tales garantías adecuadas pueden consistir en el recurso a normas corporativas vinculantes, a cláusulas tipo de protección de datos adoptadas por la Comisión o por una autoridad de control, o a cláusulas contractuales autorizadas por una autoridad de control. Esas garantías deben asegurar la observancia de requisitos de protección de datos y derechos de los interesados adecuados al tratamiento dentro de la Unión, incluida la disponibilidad por parte de los interesados de derechos exigibles y de acciones legales efectivas, lo que incluye el derecho a obtener una reparación administrativa o judicial efectiva y a reclamar una indemnización, en la Unión o en un tercer país. En particular, deben referirse al cumplimiento de los principios generales relativos al tratamiento de los datos personales y los principios de la protección de datos desde el diseño y por defecto. Las transferencias también pueden realizarlas autoridades o entidades públicas con entidades o autoridades públicas de terceros países o con organizaciones internacionales con competencias o funciones correspondientes, igualmente sobre la base de disposiciones incorporadas a acuerdos administrativos, como un memorando de entendimiento, que reconozcan derechos exigibles y efectivos a los interesados. Si las garantías figuran en acuerdos administrativos que no sean jurídicamente vinculantes se debe recabar la autorización de la autoridad de control competente.

(109) La posibilidad de que el responsable o el encargado del tratamiento recurran a cláusulas tipo de protección de datos adoptadas por la Comisión o una autoridad de control no debe obstar a que los responsables o encargados incluyan las cláusulas tipo de protección de datos en un contrato más amplio, como un contrato entre dos encargados, o a que añadan otras cláusulas o garantías adicionales, siempre que no contradigan, directa o indirectamente, las cláusulas contractuales tipo adoptadas por la Comisión o por una autoridad de control, ni mermen los derechos o las libertades fundamentales de los interesados. Se debe alentar a los responsables y encargados del tratamiento a ofrecer garantías adicionales mediante compromisos contractuales que complementen las cláusulas tipo de protección de datos.

(110) Todo grupo empresarial o unión de empresas dedicadas a una actividad económica conjunta debe tener la posibilidad de invocar normas corporativas vinculantes autorizadas para sus transferencias internacionales de la Unión a organizaciones dentro del mismo grupo empresarial o unión de empresas dedicadas a una actividad económica conjunta, siempre que tales normas corporativas incorporen todos los principios esenciales y derechos aplicables con el fin de ofrecer garantías adecuadas para las transferencias o categorías de transferencias de datos de carácter personal.

(111) Se debe establecer la posibilidad de realizar transferencias en determinadas circunstancias, de mediar el consentimiento explícito del interesado, si la transferencia es ocasional y necesaria en relación con un contrato o una reclamación, independientemente de tratarse de un procedimiento judicial o un procedimiento administrativo o extrajudicial, incluidos los procedimientos ante organismos reguladores. También se debe establecer la posibilidad de realizar transferencias cuando así lo requieran razones importantes de interés público establecidas por el Derecho de la Unión o de los Estados miembros, o cuando la transferencia se haga a partir de un registro establecido por ley y se destine a consulta por el público o por personas que tengan un interés legítimo. En este último caso la transferencia no debe afectar a la totalidad de los datos personales o de las categorías de datos incluidos en el registro y, cuando el registro esté destinado a su consulta por personas que tengan un interés legítimo, la transferencia solo debe efectuarse a petición de dichas personas o, si

estas van a ser las destinatarias, teniendo plenamente en cuenta los intereses y los derechos fundamentales del interesado.

(112) Dichas excepciones deben aplicarse en particular a las transferencias de datos requeridas y necesarias por razones importantes de interés público, por ejemplo en caso de intercambios internacionales de datos entre autoridades en el ámbito de la competencia, administraciones fiscales o aduaneras, entre autoridades de supervisión financiera, entre servicios competentes en materia de seguridad social o de sanidad pública, por ejemplo en caso contactos destinados a localizar enfermedades contagiosas o para reducir y/o eliminar el dopaje en el deporte. La transferencia de datos personales también debe considerarse lícita en caso de que sea necesaria para proteger un interés esencial para los intereses vitales del interesado o de otra persona, incluida la integridad física o la vida, si el interesado no está en condiciones de dar su consentimiento. En ausencia de una decisión de adecuación, el Derecho de la Unión o de los Estados miembros puede limitar expresamente, por razones importantes de interés público, la transferencia de categorías específicas de datos a un tercer país o a una organización internacional. Los Estados miembros deben notificar esas disposiciones a la Comisión. Puede considerarse necesaria, por una razón importante de interés público o por ser de interés vital para el interesado, toda transferencia a una organización internacional humanitaria de datos personales de un interesado que no tenga capacidad física o jurídica para dar su consentimiento, con el fin de desempeñar un cometido basado en las Convenciones de Ginebra o de conformarse al Derecho internacional humanitario aplicable en caso de conflictos armados.

(113) Las transferencias que pueden calificarse de no repetitivas y sólo se refieren a un número limitado de interesados, también han de ser posibles en caso de servir a intereses legítimos imperiosos del responsable del tratamiento, si no prevalecen sobre ellos los intereses o los derechos y libertades del interesado y el responsable ha evaluado todas las circunstancias concurrentes en la transferencia de datos. El responsable debe prestar especial atención a la naturaleza de los datos personales, la finalidad y la duración de la operación o las operaciones de tratamiento propuestas, así como la situación en el país de origen, el tercer país y el país de destino final, y ofrecer, garantías apropiadas para proteger los derechos fundamentales y las libertades de las personas físicas con respecto al tratamiento de sus datos personales. Dichas transferencias sólo deben ser posibles en casos aislados, cuando ninguno de los otros motivos para la transferencia sean aplicables. Las legítimas expectativas de la sociedad en un aumento del conocimiento se deben tener en cuenta para fines de investigación científica o histórica o fines estadísticos. El responsable debe informar de la transferencia a la autoridad de control y al interesado.

(114) En cualquier caso, cuando la Comisión no haya tomado ninguna decisión sobre el nivel adecuado de la protección de datos en un tercer país, el responsable o el encargado del tratamiento deben arbitrar soluciones que garanticen a los interesados derechos exigibles y efectivos con respecto al tratamiento de sus datos en la Unión, una vez transferidos estos, de forma que sigan beneficiándose de derechos fundamentales y garantías.

(115) Algunos países terceros adoptan leyes, reglamentaciones y otros actos jurídicos con los que se pretende regular directamente las actividades de tratamiento de personas físicas y jurídicas bajo jurisdicción de los Estados miembros. Esto puede incluir sentencias de órganos jurisdiccionales o decisiones de autoridades administrativas de terceros países que obliguen a un responsable o un encargado del tratamiento a transferir o comunicar datos personales, y que no se basen en un acuerdo internacional, como un tratado de asistencia judicial mutua, en vigor entre el tercer país requirente y la Unión o un Estado miembro. La aplicación extraterritorial de dichas leyes, reglamentaciones y otros actos jurídicos puede ser contraria al Derecho internacional e impedir la protección de las personas físicas garantizada en la Unión en virtud del presente Reglamento. Las transferencias solo deben autorizarse cuando se cumplan las condiciones del presente Reglamento relativas a las transferencias a terceros países. Tal puede ser el caso, entre otros, cuando la comunicación sea necesaria por una razón importante de interés público reconocida por el Derecho de la Unión o de los Estados miembros aplicable al responsable del tratamiento.

(116) Cuando los datos personales circulan a través de las fronteras hacia el exterior de la Unión se puede poner en mayor riesgo la capacidad de las personas físicas para ejercer

los derechos de protección de datos, en particular con el fin de protegerse contra la utilización o comunicación ilícitas de dicha información. Al mismo tiempo, es posible que las autoridades de control se vean en la imposibilidad de tramitar reclamaciones o realizar investigaciones relativas a actividades desarrolladas fuera de sus fronteras. Sus esfuerzos por colaborar en el contexto transfronterizo también pueden verse obstaculizados por poderes preventivos o correctivos insuficientes, regímenes jurídicos incoherentes y obstáculos prácticos, como la escasez de recursos. Por consiguiente, es necesario fomentar una cooperación más estrecha entre las autoridades de control encargadas de la protección de datos para ayudarlas a intercambiar información y a llevar a cabo investigaciones con sus homólogos internacionales. A fin de desarrollar mecanismos de cooperación internacional que faciliten y proporcionen asistencia internacional mutua en la ejecución de legislación en materia de protección de datos personales, la Comisión y las autoridades de control deben intercambiar información y cooperar en actividades relativas al ejercicio de sus competencias con las autoridades competentes de terceros países, sobre la base de la reciprocidad y de conformidad con el presente Reglamento.

(117) El establecimiento en los Estados miembros de autoridades de control capacitadas para desempeñar sus funciones y ejercer sus competencias con plena independencia constituye un elemento esencial de la protección de las personas físicas con respecto al tratamiento de datos de carácter personal. Los Estados miembros deben tener la posibilidad de establecer más de una autoridad de control, a fin de reflejar su estructura constitucional, organizativa y administrativa.

(118) La independencia de las autoridades de control no debe significar que dichas autoridades puedan quedar exentas de mecanismos de control o supervisión en relación con sus gastos financieros, o de control judicial.

(119) Si un Estado miembro establece varias autoridades de control, debe disponer por ley mecanismos que garanticen la participación efectiva de dichas autoridades de control en el mecanismo de coherencia. Tal Estado miembro debe, en particular, designar a la autoridad de control que actuará como punto de contacto único de cara a la participación efectiva de dichas autoridades en el citado mecanismo, garantizando así una cooperación rápida y fluida con otras autoridades de control, el Comité y la Comisión.

(120) Todas las autoridades de control deben estar dotadas de los recursos financieros y humanos, los locales y las infraestructuras que sean necesarios para la realización eficaz de sus funciones, en particular las relacionadas con la asistencia recíproca y la cooperación con otras autoridades de control de la Unión. Cada autoridad de control debe disponer de un presupuesto anual público propio, que podrá formar parte del presupuesto general del Estado o de otro ámbito nacional.

(121) Las condiciones generales aplicables al miembro o los miembros de la autoridad de control deben establecerse por ley en cada Estado miembro y disponer, en particular, que dichos miembros han de ser nombrados, por un procedimiento transparente, por el Parlamento, el Gobierno o el jefe de Estado del Estado miembro, a propuesta del Gobierno, de un miembro del Gobierno o del Parlamento o una de sus cámaras, o por un organismo independiente encargado del nombramiento en virtud del Derecho de los Estados miembros. A fin de garantizar la independencia de la autoridad de control, sus miembros deben actuar con integridad, abstenerse de cualquier acción que sea incompatible con sus funciones y no participar, mientras dure su mandato, en ninguna actividad profesional incompatible, sea o no remunerada. La autoridad de control debe tener su propio personal, seleccionado por esta o por un organismo independiente establecido por el Derecho de los Estados miembros, que esté subordinado exclusivamente al miembro o los miembros de la autoridad de control.

(122) Cada autoridad de control debe ser competente, en el territorio de su Estado miembro, para ejercer los poderes y desempeñar las funciones que se le confieran de conformidad con el presente Reglamento. Lo anterior debe abarcar, en particular, el tratamiento en el contexto de las actividades de un establecimiento del responsable o del encargado en el territorio de su Estado miembro, el tratamiento de datos personales realizado por autoridades públicas o por organismos privados que actúen en interés público, el tratamiento que afecte a interesados en su territorio, o el tratamiento realizado por un responsable o un encargado que no esté establecido en la Unión cuando sus destinatarios sean interesados residentes en su territorio. Debe incluirse el examen de reclamaciones

presentadas por un interesado, la realización de investigaciones sobre la aplicación del presente Reglamento y el fomento de la sensibilización del público acerca de los riesgos, las normas, las garantías y los derechos en relación con el tratamiento de datos personales.

(123) A fin de proteger a las personas físicas con respecto al tratamiento de sus datos personales y de facilitar la libre circulación de los datos personales en el mercado interior, las autoridades de control deben supervisar la aplicación de las disposiciones adoptadas de conformidad con el presente Reglamento y contribuir a su aplicación coherente en toda la Unión. A tal efecto, las autoridades de control deben cooperar entre ellas y con la Comisión, sin necesidad de acuerdo alguno entre Estados miembros sobre la prestación de asistencia mutua ni sobre dicha cooperación.

(124) Si el tratamiento de datos personales se realiza en el contexto de las actividades de un establecimiento de un responsable o un encargado en la Unión y el responsable o el encargado está establecido en más de un Estado miembro, o si el tratamiento en el contexto de las actividades de un único establecimiento de un responsable o un encargado en la Unión afecta o es probable que afecte sustancialmente a interesados en más de un Estado miembro, la autoridad de control del establecimiento principal o del único establecimiento del responsable o del encargado debe actuar como autoridad principal. Dicha autoridad debe cooperar con las demás autoridades interesadas, ya sea porque el responsable o el encargado tenga un establecimiento en el territorio de su Estado miembro, porque afecte sustancialmente a interesados que residen en su territorio, o porque se haya presentado una reclamación ante ellas. Asimismo, cuando un interesado que no resida en ese Estado miembro haya presentado una reclamación, la autoridad de control ante la que se haya presentado esta también debe ser autoridad de control interesada. En el marco de sus funciones de formulación de directrices sobre cualquier cuestión relacionada con la aplicación del presente Reglamento, el Comité debe estar facultado para formular directrices, en particular sobre los criterios que han de tenerse en cuenta para determinar si el tratamiento en cuestión afecta sustancialmente a interesados de más de un Estado miembro y sobre lo que constituya una objeción pertinente y motivada.

(125) La autoridad principal debe ser competente para adoptar decisiones vinculantes relativas a las medidas de aplicación de los poderes conferidos con arreglo al presente Reglamento. En su calidad de autoridad principal, la autoridad de control debe implicar estrechamente y coordinar a las autoridades de control interesadas en el proceso de toma de decisiones. En los casos en los que la decisión consista en rechazar total o parcialmente la reclamación del interesado, esa decisión debe ser adoptada por la autoridad de control ante la que se haya presentado la reclamación.

(126) La decisión debe ser acordada conjuntamente por la autoridad de control principal y las autoridades de control interesadas y debe dirigirse al establecimiento principal o único del responsable o del encargado del tratamiento y ser vinculante para ambos. El responsable o el encargado deben tomar las medidas necesarias para garantizar el cumplimiento del presente Reglamento y la aplicación de la decisión notificada por la autoridad de control principal al establecimiento principal del responsable o del encargado en lo que se refiere a las actividades de tratamiento en la Unión.

(127) Cada autoridad de control que no actúa como autoridad principal debe ser competente para tratar asuntos locales en los que, si bien el responsable o el encargado del tratamiento está establecido en más de un Estado miembro, el objeto del tratamiento específico se refiere exclusivamente al tratamiento efectuado en un único Estado miembro y afecta exclusivamente a interesados de ese único Estado miembro, por ejemplo cuando el tratamiento tiene como objeto datos personales de empleados en el contexto específico de empleo de un Estado miembro. En tales casos, la autoridad de control debe informar sin dilación al respecto a la autoridad de control principal. Una vez informada, la autoridad de control principal debe decidir si tratará el asunto de acuerdo con la disposición aplicable a la cooperación entre la autoridad de control principal y otras autoridades de control interesadas («mecanismo de ventanilla única»), o si lo debe tratar localmente la autoridad de control que le haya informado. Al decidir si trata el asunto, la autoridad de control principal debe considerar si existe un establecimiento del responsable o del encargado en el Estado miembro de la autoridad de control que le haya informado, con el fin de garantizar la ejecución efectiva de la decisión respecto del responsable o encargado del tratamiento. Si la

autoridad de control principal decide tratar el asunto, se debe ofrecer a la autoridad de control informante la posibilidad de presentar un proyecto de decisión, que la autoridad de control principal ha de tener en cuenta en la mayor medida posible al preparar su proyecto de decisión al amparo del mecanismo de ventanilla única.

(128) Las normas sobre la autoridad de control principal y el mecanismo de ventanilla única no deben aplicarse cuando el tratamiento sea realizado por autoridades públicas u organismos privados en interés público. En tales casos, la única autoridad de control competente para ejercer los poderes conferidos con arreglo al presente Reglamento debe ser la autoridad de control del Estado miembro en el que estén establecidos la autoridad pública o el organismo privado.

(129) Para garantizar la supervisión y ejecución coherentes del presente Reglamento en toda la Unión, las autoridades de control deben tener en todos los Estados miembros las mismas funciones y poderes efectivos, incluidos poderes de investigación, poderes correctivos y sancionadores, y poderes de autorización y consultivos, especialmente en casos de reclamaciones de personas físicas, y sin perjuicio de las competencias de las autoridades encargadas de la persecución de los delitos con arreglo al Derecho de los Estados miembros para poner en conocimiento de las autoridades judiciales las infracciones del presente Reglamento y ejercitar acciones judiciales. Dichos poderes deben incluir también el poder de imponer una limitación temporal o definitiva al tratamiento, incluida su prohibición. Los Estados miembros pueden especificar otras funciones relacionadas con la protección de datos personales con arreglo al presente Reglamento. Los poderes de las autoridades de control deben ejercerse de conformidad con garantías procesales adecuadas establecidas en el Derecho de la Unión y los Estados miembros, de forma imparcial, equitativa y en un plazo razonable. En particular, toda medida debe ser adecuada, necesaria y proporcionada con vistas a garantizar el cumplimiento del presente Reglamento, teniendo en cuenta las circunstancias de cada caso concreto, respetar el derecho de todas las personas a ser oídas antes de que se adopte cualquier medida que las afecte negativamente y evitar costes superfluos y molestias excesivas para las personas afectadas. Los poderes de investigación en lo que se refiere al acceso a instalaciones deben ejercerse de conformidad con los requisitos específicos del Derecho procesal de los Estados miembros, como el de la autorización judicial previa. Toda medida jurídicamente vinculante de la autoridad de control debe constar por escrito, ser clara e inequívoca, indicar la autoridad de control que dictó la medida y la fecha en que se dictó, llevar la firma del director o de un miembro de la autoridad de control autorizado por este, especificar los motivos de la medida y mencionar el derecho a la tutela judicial efectiva. Esto no debe obstar a que se impongan requisitos adicionales con arreglo al Derecho procesal de los Estados miembros. La adopción de una decisión jurídicamente vinculante implica que puede ser objeto de control judicial en el Estado miembro de la autoridad de control que adoptó la decisión.

(130) Cuando la autoridad de control ante la cual se haya presentado la reclamación no sea la autoridad de control principal, esta última debe cooperar estrechamente con la primera con arreglo a las disposiciones sobre cooperación y coherencia establecidas en el presente Reglamento. En tales casos, la autoridad de control principal, al tomar medidas concebidas para producir efectos jurídicos, incluida la imposición de multas administrativas, debe tener en cuenta en la mayor medida posible la opinión de la autoridad de control ante la cual se haya presentado la reclamación y la cual debe seguir siendo competente para realizar cualquier investigación en el territorio de su propio Estado miembro en enlace con la autoridad de control competente.

(131) En casos en los que otra autoridad de control deba actuar como autoridad de control principal para las actividades de tratamiento del responsable o del encargado pero el objeto concreto de una reclamación o la posible infracción afecta únicamente a las actividades de tratamiento del responsable o del encargado en el Estado miembro en el que se haya presentado la reclamación o detectado la posible infracción y el asunto no afecta sustancialmente ni es probable que afecte sustancialmente a interesados de otros Estados miembros, la autoridad de control que reciba una reclamación o que detecte situaciones que conlleven posibles infracciones del presente Reglamento o reciba de otra manera información sobre estas debe tratar de llegar a un arreglo amistoso con el responsable del tratamiento y, si no prospera, ejercer todos sus poderes. En lo anterior se debe incluir el

tratamiento específico realizado en el territorio del Estado miembro de la autoridad de control o con respecto a interesados en el territorio de dicho Estado miembro; el tratamiento efectuado en el contexto de una oferta de bienes o servicios destinada específicamente a interesados en el territorio del Estado miembro de la autoridad de control; o el tratamiento que deba evaluarse teniendo en cuenta las obligaciones legales pertinentes en virtud del Derecho de los Estados miembros.

(132) Entre las actividades de sensibilización del público por parte de las autoridades de control deben incluirse medidas específicas dirigidas a los responsables y los encargados del tratamiento, incluidas las microempresas y las pequeñas y medianas empresas, así como las personas físicas, en particular en el contexto educativo.

(133) Las autoridades de control se deben ayudar una a otra en el desempeño de sus funciones y prestar asistencia mutua, con el fin de garantizar la aplicación y ejecución coherentes del presente Reglamento en el mercado interior. Una autoridad de control que solicite asistencia mutua puede adoptar una medida provisional si no recibe respuesta a su solicitud de asistencia en el plazo de un mes a partir de su recepción por la otra autoridad de control.

(134) Cada autoridad de control debe participar, cuando proceda, en operaciones conjuntas con otras autoridades de control. La autoridad de control a la que se solicite ayuda debe tener la obligación de responder a la solicitud en un plazo de tiempo determinado.

(135) A fin de garantizar la aplicación coherente del presente Reglamento en toda la Unión, debe establecerse un mecanismo de coherencia para la cooperación entre las autoridades de control. Este mecanismo debe aplicarse en particular cuando una autoridad de control prevea adoptar una medida dirigida a producir efectos jurídicos en lo que se refiere a operaciones de tratamiento que afecten sustancialmente a un número significativo de interesados en varios Estados miembros. También debe aplicarse cuando cualquier autoridad de control interesada o la Comisión soliciten que dicho asunto se trate al amparo del mecanismo de coherencia. Dicho mecanismo debe entenderse sin perjuicio de cualesquiera medidas que la Comisión pueda adoptar en el ejercicio de sus poderes con arreglo a los Tratados.

(136) En aplicación del mecanismo de coherencia, el Comité debe, en un plazo determinado, emitir un dictamen, si así lo decide una mayoría de sus miembros o si así lo solicita cualquier autoridad de control interesada o la Comisión. El Comité también debe estar facultado para adoptar decisiones jurídicamente vinculantes en caso de diferencias entre autoridades de control. A tal efecto debe dictar, en principio por mayoría de dos tercios de sus miembros, decisiones jurídicamente vinculantes en casos claramente especificados en los que exista conflicto de opiniones entre las autoridades de control, en particular en el mecanismo de cooperación entre la autoridad de control principal y las autoridades de control interesadas sobre el fondo del asunto, especialmente en caso de infracción del presente Reglamento.

(137) La necesidad urgente de actuar puede obedecer a la necesidad de proteger los derechos y libertades de los interesados, en particular cuando exista el riesgo de que pueda verse considerablemente obstaculizado el reconocimiento de alguno de sus derechos. Por lo tanto, una autoridad de control debe poder adoptar en su territorio medidas provisionales, debidamente justificadas, con un plazo de validez determinado no superior a tres meses.

(138) La aplicación de tal mecanismo debe ser una condición para la licitud de una medida de una autoridad de control destinada a producir efectos jurídicos, en aquellos casos en los que su aplicación sea obligatoria. En otros casos de relevancia transfronteriza, la autoridad de control principal y las autoridades de control interesadas deben aplicar entre sí el mecanismo de cooperación, y las autoridades de control interesadas pueden prestarse asistencia mutua y realizar entre sí operaciones conjuntas, sobre una base bilateral o multilateral, sin tener que aplicarlo.

(139) A fin de fomentar la aplicación coherente del presente Reglamento, el Comité debe constituirse como organismo independiente de la Unión. Para cumplir sus objetivos, el Comité debe tener personalidad jurídica. Su presidente debe ostentar su representación. El Comité debe sustituir al Grupo de protección de las personas en lo que respecta al tratamiento de datos personales creado por la Directiva 95/46/CE. Debe estar compuesto por el director de una autoridad de control de cada Estado miembro y el Supervisor Europeo de

Protección de Datos, o por sus respectivos representantes. La Comisión debe participar en las actividades del Comité sin derecho a voto y se deben reconocer derechos de voto específicos al Supervisor Europeo de Protección de Datos. El Comité debe contribuir a la aplicación coherente del presente Reglamento en toda la Unión, entre otras cosas asesorando a la Comisión, en particular sobre el nivel de protección en terceros países u organizaciones internacionales, y fomentando la cooperación de las autoridades de control en toda la Unión. El Comité debe actuar con independencia en el cumplimiento de sus funciones.

(140) El Comité debe contar con una secretaría, a cargo el Supervisor Europeo de Protección de Datos. El personal del Supervisor Europeo de Protección de Datos que participe en la realización de las funciones conferidas al Comité por el presente Reglamento debe desempeñar sus funciones siguiendo exclusivamente las instrucciones del presidente del Comité y responder ante él.

(141) Todo interesado debe tener derecho a presentar una reclamación ante una autoridad de control única, en particular en el Estado miembro de su residencia habitual, y derecho a la tutela judicial efectiva de conformidad con el artículo 47 de la Carta si considera que se vulneran sus derechos con arreglo al presente Reglamento o en caso de que la autoridad de control no responda a una reclamación, rechace o desestime total o parcialmente una reclamación o no actúe cuando sea necesario para proteger los derechos del interesado. La investigación a raíz de una reclamación debe llevarse a cabo, bajo control judicial, si procede en el caso concreto. La autoridad de control debe informar al interesado de la evolución y el resultado de la reclamación en un plazo razonable. Si el asunto requiere una mayor investigación o coordinación con otra autoridad de control, se debe facilitar información intermedia al interesado. Para facilitar la presentación de reclamaciones, cada autoridad de control debe adoptar medidas como el suministro de un formulario de reclamaciones, que pueda cumplimentarse también por medios electrónicos, sin excluir otros medios de comunicación.

(142) El interesado que considere vulnerados los derechos reconocidos por el presente Reglamento debe tener derecho a conferir mandato a una entidad, organización o asociación sin ánimo de lucro que esté constituida con arreglo al Derecho de un Estado miembro, tenga objetivos estatutarios que sean de interés público y actúe en el ámbito de la protección de los datos personales, para que presente en su nombre una reclamación ante la autoridad de control, ejerza el derecho a la tutela judicial en nombre de los interesados o, si así lo establece el Derecho del Estado miembro, ejerza el derecho a recibir una indemnización en nombre de estos. Un Estado miembro puede reconocer a tal entidad, organización o asociación el derecho a presentar en él una reclamación con independencia del mandato de un interesado y el derecho a la tutela judicial efectiva, cuando existan motivos para creer que se han vulnerado los derechos de un interesado como consecuencia de un tratamiento de datos personales que sea contrario al presente Reglamento. Esa entidad, organización o asociación no puede estar autorizada a reclamar una indemnización en nombre de un interesado al margen del mandato de este último.

(143) Toda persona física o jurídica tiene derecho a interponer ante el Tribunal de Justicia recurso de anulación de decisiones del Comité, en las condiciones establecidas en el artículo 263 del TFUE. Como destinatarias de dichas decisiones, las autoridades de control interesadas que quieran impugnarlas tienen que interponer recurso en el plazo de dos meses a partir del momento en que les fueron notificadas, de conformidad con el artículo 263 del TFUE. En caso de que las decisiones del Comité afecten directa e individualmente a un responsable, un encargado o al reclamante, estos pueden interponer recurso de anulación de dichas decisiones en el plazo de dos meses a partir de su publicación en el sitio web del Comité, de conformidad con el artículo 263 del TFUE. Sin perjuicio de lo dispuesto en el artículo 263 del TFUE, toda persona física o jurídica debe tener derecho a la tutela judicial efectiva ante el tribunal nacional competente contra las decisiones de una autoridad de control que produzcan efectos jurídicos que le afecten. Tales decisiones se refieren en particular al ejercicio de los poderes de investigación, corrección y autorización por parte de la autoridad de control o a la desestimación o rechazo de reclamaciones. No obstante, el derecho a la tutela judicial efectiva no incluye medidas adoptadas por las autoridades de control que no sean jurídicamente vinculantes, como los dictámenes publicados o el

asesoramiento facilitado por ellas. Las acciones contra una autoridad de control deben ejercitarse ante los tribunales del Estado miembro en el que esté establecida y tramitarse con arreglo al Derecho procesal de dicho Estado miembro. Dichos tribunales deben tener plena jurisdicción, incluida la competencia para examinar todos los elementos de hecho y de Derecho relativos a la causa de la que conozcan.

Si una autoridad de control rechaza o desestima una reclamación, el reclamante puede ejercitar una acción ante los tribunales del mismo Estado miembro. En el contexto de las acciones judiciales relacionadas con la aplicación del presente Reglamento, los tribunales nacionales que estimen necesaria una decisión al respecto para poder emitir su fallo pueden, o en el caso establecido en el artículo 267 del TFUE, deben solicitar al Tribunal de Justicia que se pronuncie con carácter prejudicial sobre la interpretación del Derecho de la Unión, incluido el presente Reglamento. Además, si una decisión de una autoridad de control por la que se ejecuta una decisión del Comité se impugna ante un tribunal nacional y se cuestiona la validez de la decisión del Comité, dicho tribunal nacional no es competente para declarar inválida la decisión del Comité, sino que, si la considera inválida, tiene que remitir la cuestión de la validez al Tribunal de Justicia de conformidad con el artículo 267 del TFUE, según la interpretación de este. No obstante, un tribunal nacional puede no remitir la cuestión de la validez de la decisión del Comité a instancia de una persona física o jurídica que, habiendo tenido la oportunidad de interponer recurso de anulación de dicha decisión, en particular si dicha decisión la afectaba directa e individualmente, no lo hizo en el plazo establecido en el artículo 263 del TFUE.

(144) Si un tribunal ante el cual se ejercitaron acciones contra una decisión de una autoridad de control tiene motivos para creer que se ejercitaron acciones ante un tribunal competente de otro Estado miembro relativas al mismo tratamiento, como tener el mismo asunto con respecto a un tratamiento por el mismo responsable o encargado, o la misma causa de la acción, debe ponerse en contacto con ese tribunal para confirmar la existencia de tales acciones conexas. Si dichas acciones conexas están pendientes ante un tribunal de otro Estado miembro, cualquier otro tribunal distinto de aquel ante el cual se ejercitó la acción en primer lugar puede suspender el procedimiento o, a instancia de una de las partes, inhibirse a favor del tribunal ante el cual se ejercitó la acción en primer lugar si este último es competente para su conocimiento y su acumulación es conforme a Derecho. Se consideran conexas las acciones vinculadas entre sí por una relación tan estrecha que procede tramitarlas y resolverlas conjuntamente a fin de evitar resoluciones que podrían ser incompatibles si se sustanciaran como causas separadas.

(145) Por lo que respecta a las acciones contra los responsables o encargados del tratamiento, el reclamante debe tener la opción de ejercitarlas ante los tribunales de los Estados miembros en los que el responsable o el encargado tenga un establecimiento o resida el interesado, a menos que el responsable sea una autoridad pública de un Estado miembro que actúe en el ejercicio de poderes públicos.

(146) El responsable o el encargado del tratamiento debe indemnizar cualesquiera daños y perjuicios que pueda sufrir una persona como consecuencia de un tratamiento en infracción del presente Reglamento. El responsable o el encargado deben quedar exentos de responsabilidad si se demuestra que en modo alguno son responsables de los daños y perjuicios. El concepto de daños y perjuicios debe interpretarse en sentido amplio a la luz de la jurisprudencia del Tribunal de Justicia, de tal modo que se respeten plenamente los objetivos del presente Reglamento. Lo anterior se entiende sin perjuicio de cualquier reclamación por daños y perjuicios derivada de la vulneración de otras normas del Derecho de la Unión o de los Estados miembros. Un tratamiento en infracción del presente Reglamento también incluye aquel tratamiento que infringe actos delegados y de ejecución adoptados de conformidad con el presente Reglamento y el Derecho de los Estados miembros que especifique las normas del presente Reglamento. Los interesados deben recibir una indemnización total y efectiva por los daños y perjuicios sufridos. Si los responsables o encargados participan en el mismo tratamiento, cada responsable o encargado debe ser considerado responsable de la totalidad de los daños y perjuicios. No obstante, si se acumulan en la misma causa de conformidad con el Derecho de los Estados miembros, la indemnización puede prorratearse en función de la responsabilidad de cada responsable o encargado por los daños y perjuicios causados por el tratamiento, siempre

que se garantice la indemnización total y efectiva del interesado que sufrió los daños y perjuicios. Todo responsable o encargado que haya abonado la totalidad de la indemnización puede interponer recurso posteriormente contra otros responsables o encargados que hayan participado en el mismo tratamiento.

(147) En los casos en que el presente Reglamento contiene normas específicas sobre competencia judicial, en particular por lo que respecta a las acciones que tratan de obtener satisfacción por la vía judicial, incluida la indemnización, contra un responsable o encargado del tratamiento, las normas generales de competencia judicial como las establecidas en el Reglamento (UE) n.º 1215/2012 del Parlamento Europeo y del Consejo [13] deben entenderse sin perjuicio de la aplicación de dichas normas específicas.

(148) A fin de reforzar la aplicación de las normas del presente Reglamento, cualquier infracción de este debe ser castigada con sanciones, incluidas multas administrativas, con carácter adicional a medidas adecuadas impuestas por la autoridad de control en virtud del presente Reglamento, o en sustitución de estas. En caso de infracción leve, o si la multa que probablemente se impusiera constituyese una carga desproporcionada para una persona física, en lugar de sanción mediante multa puede imponerse un apercibimiento. Debe no obstante prestarse especial atención a la naturaleza, gravedad y duración de la infracción, a su carácter intencional, a las medidas tomadas para paliar los daños y perjuicios sufridos, al grado de responsabilidad o a cualquier infracción anterior pertinente, a la forma en que la autoridad de control haya tenido conocimiento de la infracción, al cumplimiento de medidas ordenadas contra el responsable o encargado, a la adhesión a códigos de conducta y a cualquier otra circunstancia agravante o atenuante. La imposición de sanciones, incluidas las multas administrativas, debe estar sujeta a garantías procesales suficientes conforme a los principios generales del Derecho de la Unión y de la Carta, entre ellas el derecho a la tutela judicial efectiva y a un proceso con todas las garantías.

(149) Los Estados miembros deben tener la posibilidad de establecer normas en materia de sanciones penales por infracciones del presente Reglamento, incluidas las infracciones de normas nacionales adoptadas con arreglo a él y dentro de sus límites. Dichas sanciones penales pueden asimismo autorizar la privación de los beneficios obtenidos en infracción del presente Reglamento. No obstante, la imposición de sanciones penales por infracciones de dichas normas nacionales y de sanciones administrativas no debe entrañar la vulneración del principio ne bis in idem, según la interpretación del Tribunal de Justicia.

(150) A fin de reforzar y armonizar las sanciones administrativas por infracción del presente Reglamento, cada autoridad de control debe estar facultada para imponer multas administrativas. El presente Reglamento debe indicar las infracciones así como el límite máximo y los criterios para fijar las correspondientes multas administrativas, que la autoridad de control competente debe determinar en cada caso individual teniendo en cuenta todas las circunstancias concurrentes en él, atendiendo en particular a la naturaleza, gravedad y duración de la infracción y sus consecuencias y a las medidas tomadas para garantizar el cumplimiento de las obligaciones impuestas por el presente Reglamento e impedir o mitigar las consecuencias de la infracción. Si las multas administrativas se imponen a una empresa, por tal debe entenderse una empresa con arreglo a los artículos 101 y 102 del TFUE. Si las multas administrativas se imponen a personas que no son una empresa, la autoridad de control debe tener en cuenta al valorar la cuantía apropiada de la multa el nivel general de ingresos prevaleciente en el Estado miembro así como la situación económica de la persona. El mecanismo de coherencia también puede emplearse para fomentar una aplicación coherente de las multas administrativas. Debe corresponder a los Estados miembros determinar si y en qué medida se debe imponer multas administrativas a las autoridades públicas. La imposición de una multa administrativa o de una advertencia no afecta al ejercicio de otras competencias de las autoridades de control ni a la aplicación de otras sanciones al amparo del presente Reglamento.

(151) Los ordenamientos jurídicos de Dinamarca y Estonia no permiten las multas administrativas según lo dispuesto en el presente Reglamento. Las normas sobre multas administrativas pueden ser aplicadas en Dinamarca de tal manera que la multa sea impuesta por los tribunales nacionales competentes en cuanto sanción penal, y en Estonia de tal manera que la multa sea impuesta por la autoridad de control en el marco de un juicio de faltas, siempre que tal aplicación de las normas en dichos Estados miembros tenga un efecto

equivalente a las multas administrativas impuestas por las autoridades de control. Por lo tanto los tribunales nacionales competentes deben tener en cuenta la recomendación de la autoridad de control que incoe la multa. En todo caso, las multas impuestas deben ser efectivas, proporcionadas y disuasorias.

(152) En los casos en que el presente Reglamento no armoniza las sanciones administrativas, o en otros casos en que se requiera, por ejemplo en casos de infracciones graves del presente Reglamento, los Estados miembros deben aplicar un sistema que establezca sanciones efectivas, proporcionadas y disuasorias. La naturaleza de dichas sanciones, ya sea penal o administrativa, debe ser determinada por el Derecho de los Estados miembros.

(153) El Derecho de los Estados miembros debe conciliar las normas que rigen la libertad de expresión e información, incluida la expresión periodística, académica, artística o literaria, con el derecho a la protección de los datos personales con arreglo al presente Reglamento. El tratamiento de datos personales con fines exclusivamente periodísticos o con fines de expresión académica, artística o literaria debe estar sujeto a excepciones o exenciones de determinadas disposiciones del presente Reglamento si así se requiere para conciliar el derecho a la protección de los datos personales con el derecho a la libertad de expresión y de información consagrado en el artículo 11 de la Carta. Esto debe aplicarse en particular al tratamiento de datos personales en el ámbito audiovisual y en los archivos de noticias y hemerotecas. Por tanto, los Estados miembros deben adoptar medidas legislativas que establezcan las exenciones y excepciones necesarias para equilibrar estos derechos fundamentales. Los Estados miembros deben adoptar tales exenciones y excepciones con relación a los principios generales, los derechos del interesado, el responsable y el encargado del tratamiento, la transferencia de datos personales a terceros países u organizaciones internacionales, las autoridades de control independientes, la cooperación y la coherencia, y las situaciones específicas de tratamiento de datos. Si dichas exenciones o excepciones difieren de un Estado miembro a otro debe regir el Derecho del Estado miembro que sea aplicable al responsable del tratamiento. A fin de tener presente la importancia del derecho a la libertad de expresión en toda sociedad democrática, es necesario que nociones relativas a dicha libertad, como el periodismo, se interpreten en sentido amplio.

(154) El presente Reglamento permite que, al aplicarlo, se tenga en cuenta el principio de acceso del público a los documentos oficiales. El acceso del público a documentos oficiales puede considerarse de interés público. Los datos personales de documentos que se encuentren en poder de una autoridad pública o un organismo público deben poder ser comunicados públicamente por dicha autoridad u organismo si así lo establece el Derecho de la Unión o los Estados miembros aplicable a dicha autoridad u organismo. Ambos Derechos deben conciliar el acceso del público a documentos oficiales y la reutilización de la información del sector público con el derecho a la protección de los datos personales y, por tanto, pueden establecer la necesaria conciliación con el derecho a la protección de los datos personales de conformidad con el presente Reglamento. La referencia a autoridades y organismos públicos debe incluir, en este contexto, a todas las autoridades u otros organismos a los que se aplica el Derecho de los Estados miembros sobre el acceso del público a documentos. La Directiva 2003/98/CE del Parlamento Europeo y del Consejo [(14)] no altera ni afecta en modo alguno al nivel de protección de las personas físicas con respecto al tratamiento de datos personales con arreglo a las disposiciones del Derecho de la Unión y los Estados miembros y, en particular, no altera las obligaciones ni los derechos establecidos en el presente Reglamento. En concreto, dicha Directiva no debe aplicarse a los documentos a los que no pueda accederse o cuyo acceso esté limitado en virtud de regímenes de acceso por motivos de protección de datos personales, ni a partes de documentos accesibles en virtud de dichos regímenes que contengan datos personales cuya reutilización haya quedado establecida por ley como incompatible con el Derecho relativo a la protección de las personas físicas con respecto al tratamiento de los datos personales.

(155) El Derecho de los Estados miembros o los convenios colectivos, incluidos los «convenios de empresa», pueden establecer normas específicas relativas al tratamiento de datos personales de los trabajadores en el ámbito laboral, en particular en relación con las condiciones en las que los datos personales en el contexto laboral pueden ser objeto de tratamiento sobre la base del consentimiento del trabajador, los fines de la contratación, la

ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por convenio colectivo, la gestión, planificación y organización del trabajo, la igualdad y seguridad en el lugar de trabajo, la salud y seguridad en el trabajo, así como a los fines del ejercicio y disfrute, sea individual o colectivo, de derechos y prestaciones relacionados con el empleo y a efectos de la rescisión de la relación laboral.

(156) El tratamiento de datos personales con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos debe estar supeditado a unas garantías adecuadas para los derechos y libertades del interesado de conformidad con el presente Reglamento. Esas garantías deben asegurar que se aplican medidas técnicas y organizativas para que se observe, en particular, el principio de minimización de los datos. El tratamiento ulterior de datos personales con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos ha de efectuarse cuando el responsable del tratamiento haya evaluado la viabilidad de cumplir esos fines mediante un tratamiento de datos que no permita identificar a los interesados, o que ya no lo permita, siempre que existan las garantías adecuadas (como, por ejemplo, la seudonimización de datos). Los Estados miembros deben establecer garantías adecuadas para el tratamiento de datos personales con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos. Debe autorizarse que los Estados miembros establezcan, bajo condiciones específicas y a reserva de garantías adecuadas para los interesados, especificaciones y excepciones con respecto a los requisitos de información y los derechos de rectificación, de supresión, al olvido, de limitación del tratamiento, a la portabilidad de los datos y de oposición, cuando se traten datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos. Las condiciones y garantías en cuestión pueden conllevar procedimientos específicos para que los interesados ejerzan dichos derechos si resulta adecuado a la luz de los fines perseguidos por el tratamiento específico, junto con las medidas técnicas y organizativas destinadas a minimizar el tratamiento de datos personales atendiendo a los principios de proporcionalidad y necesidad. El tratamiento de datos personales con fines científicos también debe observar otras normas pertinentes, como las relativas a los ensayos clínicos.

(157) Combinando información procedente de registros, los investigadores pueden obtener nuevos conocimientos de gran valor sobre condiciones médicas extendidas, como las enfermedades cardiovasculares, el cáncer y la depresión. Partiendo de registros, los resultados de las investigaciones pueden ser más sólidos, ya que se basan en una población mayor. Dentro de las ciencias sociales, la investigación basada en registros permite que los investigadores obtengan conocimientos esenciales acerca de la correlación a largo plazo, con otras condiciones de vida, de diversas condiciones sociales, como el desempleo y la educación. Los resultados de investigaciones obtenidos de registros proporcionan conocimientos sólidos y de alta calidad que pueden servir de base para la concepción y ejecución de políticas basada en el conocimiento, mejorar la calidad de vida de numerosas personas y mejorar la eficiencia de los servicios sociales. Para facilitar la investigación científica, los datos personales pueden tratarse con fines científicos, a reserva de condiciones y garantías adecuadas establecidas en el Derecho de la Unión o de los Estados miembros.

(158) El presente Reglamento también debe aplicarse al tratamiento de datos personales realizado con fines de archivo, teniendo presente que no debe se de aplicación a personas fallecidas. Las autoridades públicas o los organismos públicos o privados que llevan registros de interés público deben ser servicios que están obligados, con arreglo al Derecho de la Unión o de los Estados miembros, a adquirir, mantener, evaluar, organizar, describir, comunicar, promover y difundir registros de valor perdurable para el interés público general y facilitar acceso a ellos. Los Estados miembros también debe estar autorizados a establecer el tratamiento ulterior de datos personales con fines de archivo, por ejemplo a fin de ofrecer información específica relacionada con el comportamiento político bajo antiguos regímenes de Estados totalitarios, el genocidio, los crímenes contra la humanidad, en particular el Holocausto, o los crímenes de guerra.

(159) El presente Reglamento también debe aplicarse al tratamiento datos personales que se realice con fines de investigación científica. El tratamiento de datos personales con fines de investigación científica debe interpretarse, a efectos del presente Reglamento, de

manera amplia, que incluya, por ejemplo, el desarrollo tecnológico y la demostración, la investigación fundamental, la investigación aplicada y la investigación financiada por el sector privado. Además, debe tener en cuenta el objetivo de la Unión establecido en el artículo 179, apartado 1, del TFUE de realizar un espacio europeo de investigación. Entre los fines de investigación científica también se deben incluir los estudios realizados en interés público en el ámbito de la salud pública. Para cumplir las especificidades del tratamiento de datos personales con fines de investigación científica deben aplicarse condiciones específicas, en particular en lo que se refiere a la publicación o la comunicación de otro modo de datos personales en el contexto de fines de investigación científica. Si el resultado de la investigación científica, en particular en el ámbito de la salud, justifica otras medidas en beneficio del interesado, las normas generales del presente Reglamento deben aplicarse teniendo en cuenta tales medidas.

(160) El presente Reglamento debe aplicarse asimismo al tratamiento datos personales que se realiza con fines de investigación histórica. Esto incluye asimismo la investigación histórica y la investigación para fines genealógicos, teniendo en cuenta que el presente Reglamento no es de aplicación a personas fallecidas.

(161) Al objeto de otorgar el consentimiento para la participación en actividades de investigación científica en ensayos clínicos, deben aplicarse las disposiciones pertinentes del Reglamento (UE) n.º 536/2014 del Parlamento Europeo y del Consejo [15].

(162) El presente Reglamento debe aplicarse al tratamiento de datos personales con fines estadísticos. El contenido estadístico, el control de accesos, las especificaciones para el tratamiento de datos personales con fines estadísticos y las medidas adecuadas para salvaguardar los derechos y las libertades de los interesados y garantizar la confidencialidad estadística deben ser establecidos, dentro de los límites del presente Reglamento, por el Derecho de la Unión o de los Estados miembros. Por fines estadísticos se entiende cualquier operación de recogida y tratamiento de datos personales necesarios para encuestas estadísticas o para la producción de resultados estadísticos. Estos resultados estadísticos pueden además utilizarse con diferentes fines, incluidos fines de investigación científica. El fin estadístico implica que el resultado del tratamiento con fines estadísticos no sean datos personales, sino datos agregados, y que este resultado o los datos personales no se utilicen para respaldar medidas o decisiones relativas a personas físicas concretas.

(163) Debe protegerse la información confidencial que las autoridades estadísticas de la Unión y nacionales recojan para la elaboración de las estadísticas oficiales europeas y nacionales. Las estadísticas europeas deben desarrollarse, elaborarse y difundirse con arreglo a los principios estadísticos fijados en el artículo 338, apartado 2, del TFUE, mientras que las estadísticas nacionales deben cumplir asimismo el Derecho de los Estados miembros. El Reglamento (CE) n.º 223/2009 del Parlamento Europeo y del Consejo [16] facilita especificaciones adicionales sobre la confidencialidad estadística aplicada a las estadísticas europeas.

(164) Por lo que respecta a los poderes de las autoridades de control para obtener del responsable o del encargado del tratamiento acceso a los datos personales y a sus locales, los Estados miembros pueden adoptar por ley, dentro de los límites fijados por el presente Reglamento, normas específicas con vistas a salvaguardar el deber de secreto profesional u obligaciones equivalentes, en la medida necesaria para conciliar el derecho a la protección de los datos personales con el deber de secreto profesional. Lo anterior se entiende sin perjuicio de las obligaciones existentes para los Estados miembros de adoptar normas sobre el secreto profesional cuando así lo exija el Derecho de la Unión.

(165) El presente Reglamento respeta y no prejuzga el estatuto reconocido en los Estados miembros, en virtud del Derecho constitucional, a las iglesias y las asociaciones o comunidades religiosas, tal como se reconoce en el artículo 17 del TFUE.

(166) A fin de cumplir los objetivos del presente Reglamento, a saber, proteger los derechos y las libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales, y garantizar la libre circulación de los datos personales en la Unión, debe delegarse en la Comisión el poder de adoptar actos de conformidad con el artículo 290 del TFUE. En particular, deben adoptarse actos delegados en relación con los criterios y requisitos para los mecanismos de certificación, la información que debe presentarse mediante iconos normalizados y los procedimientos para proporcionar

dichos iconos. Reviste especial importancia que la Comisión lleve a cabo las consultas oportunas durante la fase preparatoria, en particular con expertos. Al preparar y redactar los actos delegados, la Comisión debe garantizar la transmisión simultánea, oportuna y apropiada de los documentos pertinentes al Parlamento Europeo y al Consejo.

(167) A fin de garantizar condiciones uniformes de ejecución del presente Reglamento, deben conferirse a la Comisión competencias de ejecución cuando así lo establezca el presente Reglamento. Dichas competencias deben ejercerse de conformidad con el Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo. En este contexto, la Comisión debe considerar la adopción de medidas específicas para las microempresas y las pequeñas y medianas empresas.

(168) El procedimiento de examen debe seguirse para la adopción de actos de ejecución sobre cláusulas contractuales tipo entre responsables y encargados del tratamiento y entre responsables del tratamiento; códigos de conducta; normas técnicas y mecanismos de certificación; el nivel adecuado de protección ofrecido por un tercer país, un territorio o un sector específico en ese tercer país, o una organización internacional; cláusulas tipo de protección; formatos y procedimientos para el intercambio de información entre responsables, encargados y autoridades de control respecto de normas corporativas vinculantes; asistencia mutua; y modalidades de intercambio de información por medios electrónicos entre las autoridades de control, y entre las autoridades de control y el Comité.

(169) La Comisión debe adoptar actos de ejecución inmediatamente aplicables cuando las pruebas disponibles muestren que un tercer país, un territorio o un sector específico en ese tercer país, o una organización internacional no garantizan un nivel de protección adecuado y así lo requieran razones imperiosas de urgencia.

(170) Dado que el objetivo del presente Reglamento, a saber, garantizar un nivel equivalente de protección de las personas físicas y la libre circulación de datos personales en la Unión Europea, no puede ser alcanzado de manera suficiente por los Estados miembros, sino que, debido a las dimensiones o los efectos de la acción, puede lograrse mejor a escala de la Unión, esta puede adoptar medidas, de acuerdo con el principio de subsidiariedad establecido en el artículo 5 del Tratado de la Unión Europea (TUE). De conformidad con el principio de proporcionalidad establecido en el mismo artículo, el presente Reglamento no excede de lo necesario para alcanzar dicho objetivo.

(171) La Directiva 95/46/CE debe ser derogada por el presente Reglamento. Todo tratamiento ya iniciado en la fecha de aplicación del presente Reglamento debe ajustarse al presente Reglamento en el plazo de dos años a partir de la fecha de su entrada en vigor. Cuando el tratamiento se base en el consentimiento de conformidad con la Directiva 95/46/CE, no es necesario que el interesado dé su consentimiento de nuevo si la forma en que se dio el consentimiento se ajusta a las condiciones del presente Reglamento, a fin de que el responsable pueda continuar dicho tratamiento tras la fecha de aplicación del presente Reglamento. Las decisiones de la Comisión y las autorizaciones de las autoridades de control basadas en la Directiva 95/46/CE permanecen en vigor hasta que sean modificadas, sustituidas o derogadas.

(172) De conformidad con el artículo 28, apartado 2, del Reglamento (CE) n.º 45/2001, se consultó al Supervisor Europeo de Protección de Datos, y éste emitió su dictamen el 7 de marzo de 2012 [17].

(173) El presente Reglamento debe aplicarse a todas las cuestiones relativas a la protección de los derechos y las libertades fundamentales en relación con el tratamiento de datos personales que no están sujetas a obligaciones específicas con el mismo objetivo establecidas en la Directiva 2002/58/CE del Parlamento Europeo y del Consejo [18], incluidas las obligaciones del responsable del tratamiento y los derechos de las personas físicas. Para aclarar la relación entre el presente Reglamento y la Directiva 2002/58/CE, esta última debe ser modificada en consecuencia. Una vez que se adopte el presente Reglamento, debe revisarse la Directiva 2002/58/CE, en particular con objeto de garantizar la coherencia con el presente Reglamento.

HAN ADOPTADO EL PRESENTE REGLAMENTO

---

(1) DO C 229 de 31.7.2012, p. 90.

(2) DO C 391 de 18.12.2012, p. 127.

(3) Posición del Parlamento Europeo de 12 de marzo de 2014 (pendiente de publicación en el Diario Oficial) y posición del Consejo en primera lectura de 8 de abril de 2016 (pendiente de publicación en el Diario Oficial). Posición del Parlamento Europeo de 14 de abril de 2016.

(4) Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO L 281 de 23.11.1995, p. 31).

(5) Recomendación de la Comisión de 6 de mayo de 2003 sobre la definición de microempresas, pequeñas y medianas empresas [C(2003) 1422] (DO L 124 de 20.5.2003, p. 36).

(6) Reglamento (CE) n.º 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (DO L 8 de 12.1.2001, p. 1).

(7) Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (véase la página 89 del presente Diario Oficial).

(8) Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico) (DO L 178 de 17.7.2000, p. 1).

(9) Directiva 2011/24/UE del Parlamento Europeo y del Consejo, de 9 de marzo de 2011, relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza (DO L 88 de 4.4.2011, p. 45).

(10) Directiva 93/13/CEE del Consejo, de 5 de abril de 1993, sobre las cláusulas abusivas en los contratos celebrados con consumidores (DO L 95 de 21.4.1993, p. 29).

(11) Reglamento (CE) n.º 1338/2008 del Parlamento Europeo y del Consejo, de 16 de diciembre de 2008, sobre estadísticas comunitarias de salud pública y de salud y seguridad en el trabajo (DO L 354 de 31.12.2008, p. 70).

(12) Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo, de 16 de febrero de 2011, por el que se establecen las normas y los principios generales relativos a las modalidades de control por parte de los Estados miembros del ejercicio de las competencias de ejecución por la Comisión (DO L 55 de 28.2.2011, p. 13).

(13) Reglamento (UE) n.º 1215/2012 del Parlamento Europeo y del Consejo, de 12 de diciembre de 2012, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil (DO L 351 de 20.12.2012, p. 1).

(14) Directiva 2003/98/CE del Parlamento Europeo y del Consejo, de 17 de noviembre de 2003, relativa a la reutilización de la información del sector público (DO L 345 de 31.12.2003, p. 90).

(15) Reglamento (UE) n.º 536/2014 del Parlamento Europeo y del Consejo, de 16 de abril de 2014, sobre los ensayos clínicos de medicamentos de uso humano, y por el que se deroga la Directiva 2001/20/CE (DO L 158 de 27.5.2014, p. 1).

(16) Reglamento (CE) n.º 223/2009 del Parlamento Europeo y del Consejo, de 11 de marzo de 2009, relativo a la estadística europea y por el que se deroga el Reglamento (CE, Euratom) n.º 1101/2008 relativo a la transmisión a la Oficina Estadística de las Comunidades Europeas de las informaciones amparadas por el secreto estadístico, el Reglamento (CE) n.º 322/97 del Consejo sobre la estadística comunitaria y la Decisión 89/382/CEE, Euratom del Consejo por la que se crea un Comité del programa estadístico de las Comunidades Europeas (DO L 87 de 31.3.2009, p. 164).

(17) DO C 192 de 30.6.2012, p. 7.

(18) Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) (DO L 201 de 31.7.2002, p. 37).

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

1. El presente Reglamento establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos.

2. El presente Reglamento protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales.

3. La libre circulación de los datos personales en la Unión no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales.

Artículo 2. *Ámbito de aplicación material.*

1. El presente Reglamento se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.
2. El presente Reglamento no se aplica al tratamiento de datos personales:

a) en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión;
b) por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del TUE;
c) efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas;
d) por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención.

3. El Reglamento (CE) n.º 45/2001 es de aplicación al tratamiento de datos de carácter personal por parte de las instituciones, órganos y organismos de la Unión. El Reglamento (CE) n.º 45/2001 y otros actos jurídicos de la Unión aplicables a dicho tratamiento de datos de carácter personal se adaptarán a los principios y normas del presente Reglamento de conformidad con su artículo 98.
4. El presente Reglamento se entenderá sin perjuicio de la aplicación de la Directiva 2000/31/CE, en particular sus normas relativas a la responsabilidad de los prestadores de servicios intermediarios establecidas en sus artículos 12 a 15.

Artículo 3. *Ámbito territorial.*

1. El presente Reglamento se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no.
2. El presente Reglamento se aplica al tratamiento de datos personales de interesados que se encuentren en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con:

a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o
b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión.

3. El presente Reglamento se aplica al tratamiento de datos personales por parte de un responsable que no esté establecido en la Unión sino en un lugar en que el Derecho de los Estados miembros sea de aplicación en virtud del Derecho internacional público.

Artículo 4. *Definiciones.*

A efectos del presente Reglamento se entenderá por:

1) «datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;
2) «tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o

cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;

3) «limitación del tratamiento»: el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro;

4) «elaboración de perfiles»: toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física;

5) «seudonimización»: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable;

6) «fichero»: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica;

7) «responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros;

8) «encargado del tratamiento» o «encargado»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;

9) «destinatario»: la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento;

10) «tercero»: persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado;

11) «consentimiento del interesado»: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen;

12) «violación de la seguridad de los datos personales»: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos;

13) «datos genéticos»: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona;

14) «datos biométricos»: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos;

15) «datos relativos a la salud»: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud;

16) «establecimiento principal»:

a) en lo que se refiere a un responsable del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión, salvo que las

decisiones sobre los fines y los medios del tratamiento se tomen en otro establecimiento del responsable en la Unión y este último establecimiento tenga el poder de hacer aplicar tales decisiones, en cuyo caso el establecimiento que haya adoptado tales decisiones se considerará establecimiento principal;

b) en lo que se refiere a un encargado del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión o, si careciera de esta, el establecimiento del encargado en la Unión en el que se realicen las principales actividades de tratamiento en el contexto de las actividades de un establecimiento del encargado en la medida en que el encargado esté sujeto a obligaciones específicas con arreglo al presente Reglamento;

17) «representante»: persona física o jurídica establecida en la Unión que, habiendo sido designada por escrito por el responsable o el encargado del tratamiento con arreglo al artículo 27, represente al responsable o al encargado en lo que respecta a sus respectivas obligaciones en virtud del presente Reglamento;

18) «empresa»: persona física o jurídica dedicada a una actividad económica, independientemente de su forma jurídica, incluidas las sociedades o asociaciones que desempeñen regularmente una actividad económica;

19) «grupo empresarial»: grupo constituido por una empresa que ejerce el control y sus empresas controladas;

20) «normas corporativas vinculantes»: las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta;

21) «autoridad de control»: la autoridad pública independiente establecida por un Estado miembro con arreglo a lo dispuesto en el artículo 51;

22) «autoridad de control interesada»: la autoridad de control a la que afecta el tratamiento de datos personales debido a que:

a) el responsable o el encargado del tratamiento está establecido en el territorio del Estado miembro de esa autoridad de control;

b) los interesados que residen en el Estado miembro de esa autoridad de control se ven sustancialmente afectados o es probable que se vean sustancialmente afectados por el tratamiento, o

c) se ha presentado una reclamación ante esa autoridad de control;

23) «tratamiento transfronterizo»:

a) el tratamiento de datos personales realizado en el contexto de las actividades de establecimientos en más de un Estado miembro de un responsable o un encargado del tratamiento en la Unión, si el responsable o el encargado está establecido en más de un Estado miembro, o

b) el tratamiento de datos personales realizado en el contexto de las actividades de un único establecimiento de un responsable o un encargado del tratamiento en la Unión, pero que afecta sustancialmente o es probable que afecte sustancialmente a interesados en más de un Estado miembro;

24) «objeción pertinente y motivada»: la objeción a una propuesta de decisión sobre la existencia o no de infracción del presente Reglamento, o sobre la conformidad con el presente Reglamento de acciones previstas en relación con el responsable o el encargado del tratamiento, que demuestre claramente la importancia de los riesgos que entraña el proyecto de decisión para los derechos y libertades fundamentales de los interesados y, en su caso, para la libre circulación de datos personales dentro de la Unión;

25) «servicio de la sociedad de la información»: todo servicio conforme a la definición del artículo 1, apartado 1, letra b), de la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo [(19)];

26) «organización internacional»: una organización internacional y sus entes subordinados de Derecho internacional público o cualquier otro organismo creado mediante un acuerdo entre dos o más países o en virtud de tal acuerdo.

---

[19] Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo, de 9 de septiembre de 2015, por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información (DO L 241 de 17.9.2015, p. 1).

CAPÍTULO II

Principios

Artículo 5. *Principios relativos al tratamiento.*

1. Los datos personales serán:

a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);

b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»);

c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);

d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);

e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).

2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).

Artículo 6. *Licitud del tratamiento.*

1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;

b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;

c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;

d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;

e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;

f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no

prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.

2. Los Estados miembros podrán mantener o introducir disposiciones más específicas a fin de adaptar la aplicación de las normas del presente Reglamento con respecto al tratamiento en cumplimiento del apartado 1, letras c) y e), fijando de manera más precisa requisitos específicos de tratamiento y otras medidas que garanticen un tratamiento lícito y equitativo, con inclusión de otras situaciones específicas de tratamiento a tenor del capítulo IX.

3. La base del tratamiento indicado en el apartado 1, letras c) y e), deberá ser establecida por:

a) el Derecho de la Unión, o

b) el Derecho de los Estados miembros que se aplique al responsable del tratamiento.

La finalidad del tratamiento deberá quedar determinada en dicha base jurídica o, en lo relativo al tratamiento a que se refiere el apartado 1, letra e), será necesaria para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Dicha base jurídica podrá contener disposiciones específicas para adaptar la aplicación de normas del presente Reglamento, entre otras: las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los interesados afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento, incluidas las medidas para garantizar un tratamiento lícito y equitativo, como las relativas a otras situaciones específicas de tratamiento a tenor del capítulo IX. El Derecho de la Unión o de los Estados miembros cumplirá un objetivo de interés público y será proporcional al fin legítimo perseguido.

4. Cuando el tratamiento para otro fin distinto de aquel para el que se recogieron los datos personales no esté basado en el consentimiento del interesado o en el Derecho de la Unión o de los Estados miembros que constituya una medida necesaria y proporcional en una sociedad democrática para salvaguardar los objetivos indicados en el artículo 23, apartado 1, el responsable del tratamiento, con objeto de determinar si el tratamiento con otro fin es compatible con el fin para el cual se recogieron inicialmente los datos personales, tendrá en cuenta, entre otras cosas:

a) cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento ulterior previsto;

b) el contexto en que se hayan recogido los datos personales, en particular por lo que respecta a la relación entre los interesados y el responsable del tratamiento;

c) la naturaleza de los datos personales, en concreto cuando se traten categorías especiales de datos personales, de conformidad con el artículo 9, o datos personales relativos a condenas e infracciones penales, de conformidad con el artículo 10;

d) las posibles consecuencias para los interesados del tratamiento ulterior previsto;

e) la existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización.

Artículo 7. *Condiciones para el consentimiento.*

1. Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales.

2. Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento.

3. El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el

consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo.

4. Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato.

Artículo 8. *Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información.*

1. Cuando se aplique el artículo 6, apartado 1, letra a), en relación con la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó.

Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años.

2. El responsable del tratamiento hará esfuerzos razonables para verificar en tales casos que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño, teniendo en cuenta la tecnología disponible.

3. El apartado 1 no afectará a las disposiciones generales del Derecho contractual de los Estados miembros, como las normas relativas a la validez, formación o efectos de los contratos en relación con un niño.

Artículo 9. *Tratamiento de categorías especiales de datos personales.*

1. Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física.

2. El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:

a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;

b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión o de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;

c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;

d) el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados;

e) el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos;

f) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;

g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;

h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;

i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional,

j) el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

3. Los datos personales a que se refiere el apartado 1 podrán tratarse a los fines citados en el apartado 2, letra h), cuando su tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con el Derecho de la Unión o de los Estados miembros o con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de secreto de acuerdo con el Derecho de la Unión o de los Estados miembros o de las normas establecidas por los organismos nacionales competentes.

4. Los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud.

Artículo 10. *Tratamiento de datos personales relativos a condenas e infracciones penales.*

El tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas sobre la base del artículo 6, apartado 1, sólo podrá llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la Unión o de los Estados miembros que establezca garantías adecuadas para los derechos y libertades de los interesados. Solo podrá llevarse un registro completo de condenas penales bajo el control de las autoridades públicas.

Artículo 11. *Tratamiento que no requiere identificación.*

1. Si los fines para los cuales un responsable trata datos personales no requieren o ya no requieren la identificación de un interesado por el responsable, este no estará obligado a mantener, obtener o tratar información adicional con vistas a identificar al interesado con la única finalidad de cumplir el presente Reglamento.

2. Cuando, en los casos a que se refiere el apartado 1 del presente artículo, el responsable sea capaz de demostrar que no está en condiciones de identificar al interesado, le informará en consecuencia, de ser posible. En tales casos no se aplicarán los artículos 15 a 20, excepto cuando el interesado, a efectos del ejercicio de sus derechos en virtud de dichos artículos, facilite información adicional que permita su identificación.

CAPÍTULO III

Derechos del interesado

Sección 1. Transparencia y modalidades

Artículo 12. *Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado.*

1. El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información indicada en los artículos 13 y 14, así como cualquier comunicación con arreglo a los artículos 15 a 22 y 34 relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios.

2. El responsable del tratamiento facilitará al interesado el ejercicio de sus derechos en virtud de los artículos 15 a 22. En los casos a que se refiere el artículo 11, apartado 2, el responsable no se negará a actuar a petición del interesado con el fin de ejercer sus derechos en virtud de los artículos 15 a 22, salvo que pueda demostrar que no está en condiciones de identificar al interesado.

3. El responsable del tratamiento facilitará al interesado información relativa a sus actuaciones sobre la base de una solicitud con arreglo a los artículos 15 a 22, sin dilación indebida y, en cualquier caso, en el plazo de un mes a partir de la recepción de la solicitud. Dicho plazo podrá prorrogarse otros dos meses en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes. El responsable informará al interesado de cualquiera de dichas prórrogas en el plazo de un mes a partir de la recepción de la solicitud, indicando los motivos de la dilación. Cuando el interesado presente la solicitud por medios electrónicos, la información se facilitará por medios electrónicos cuando sea posible, a menos que el interesado solicite que se facilite de otro modo.

4. Si el responsable del tratamiento no da curso a la solicitud del interesado, le informará sin dilación, y a más tardar transcurrido un mes de la recepción de la solicitud, de las razones de su no actuación y de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales.

5. La información facilitada en virtud de los artículos 13 y 14 así como toda comunicación y cualquier actuación realizada en virtud de los artículos 15 a 22 y 34 serán a título gratuito. Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, el responsable del tratamiento podrá:

a) cobrar un canon razonable en función de los costes administrativos afrontados para facilitar la información o la comunicación o realizar la actuación solicitada, o

b) negarse a actuar respecto de la solicitud.

El responsable del tratamiento soportará la carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud.

6. Sin perjuicio de lo dispuesto en el artículo 11, cuando el responsable del tratamiento tenga dudas razonables en relación con la identidad de la persona física que cursa la solicitud a que se refieren los artículos 15 a 21, podrá solicitar que se facilite la información adicional necesaria para confirmar la identidad del interesado.

7. La información que deberá facilitarse a los interesados en virtud de los artículos 13 y 14 podrá transmitirse en combinación con iconos normalizados que permitan proporcionar de forma fácilmente visible, inteligible y claramente legible una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presenten en formato electrónico serán legibles mecánicamente.

8. La Comisión estará facultada para adoptar actos delegados de conformidad con el artículo 92 a fin de especificar la información que se ha de presentar a través de iconos y los procedimientos para proporcionar iconos normalizados.

Sección 2. Información y acceso a los datos personales

Artículo 13. *Información que deberá facilitarse cuando los datos personales se obtengan del interesado.*

1. Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:

a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;
b) los datos de contacto del delegado de protección de datos, en su caso;
c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;
d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero;
e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;
f) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al lugar en que se hayan puesto a disposición.

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:

a) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;
b) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;
c) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;
d) el derecho a presentar una reclamación ante una autoridad de control;
e) si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de no facilitar tales datos;
f) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

3. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2.
4. Las disposiciones de los apartados 1, 2 y 3 no serán aplicables cuando y en la medida en que el interesado ya disponga de la información.

Artículo 14. *Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado.*

1. Cuando los datos personales no se hayan obtenidos del interesado, el responsable del tratamiento le facilitará la siguiente información:

a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;

b) los datos de contacto del delegado de protección de datos, en su caso;
c) los fines del tratamiento a que se destinan los datos personales, así como la base jurídica del tratamiento;
d) las categorías de datos personales de que se trate;
e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;
f) en su caso, la intención del responsable de transferir datos personales a un destinatario en un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al lugar en que se hayan puesto a disposición.

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente respecto del interesado:

a) el plazo durante el cual se conservarán los datos personales o, cuando eso no sea posible, los criterios utilizados para determinar este plazo;
b) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable del tratamiento o de un tercero;
c) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, y a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;
d) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basada en el consentimiento antes de su retirada;
e) el derecho a presentar una reclamación ante una autoridad de control;
f) la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público;
g) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

3. El responsable del tratamiento facilitará la información indicada en los apartados 1 y 2:

a) dentro de un plazo razonable, una vez obtenidos los datos personales, y a más tardar dentro de un mes, habida cuenta de las circunstancias específicas en las que se traten dichos datos;
b) si los datos personales han de utilizarse para comunicación con el interesado, a más tardar en el momento de la primera comunicación a dicho interesado, o
c) si está previsto comunicarlos a otro destinatario, a más tardar en el momento en que los datos personales sean comunicados por primera vez.

4. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de los datos personales para un fin que no sea aquel para el que se obtuvieron, proporcionará al interesado, antes de dicho tratamiento ulterior, información sobre ese otro fin y cualquier otra información pertinente indicada en el apartado 2.
5. Las disposiciones de los apartados 1 a 4 no serán aplicables cuando y en la medida en que:

a) el interesado ya disponga de la información;
b) la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado, en particular para el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, a reserva de las condiciones y garantías indicadas en el artículo 89, apartado 1, o en la medida en que la obligación mencionada en el apartado 1 del presente artículo pueda imposibilitar u obstaculizar gravemente el logro de los objetivos de tal tratamiento. En tales casos, el responsable adoptará medidas adecuadas para proteger los derechos, libertades e intereses legítimos del interesado, inclusive haciendo pública la información;

c) la obtención o la comunicación esté expresamente establecida por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca medidas adecuadas para proteger los intereses legítimos del interesado, o

d) cuando los datos personales deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional regulada por el Derecho de la Unión o de los Estados miembros, incluida una obligación de secreto de naturaleza legal.

Artículo 15. *Derecho de acceso del interesado.*

1. El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a la siguiente información:

a) los fines del tratamiento;

b) las categorías de datos personales de que se trate;

c) los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros países u organizaciones internacionales;

d) de ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo;

e) la existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento;

f) el derecho a presentar una reclamación ante una autoridad de control;

g) cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen;

h) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

2. Cuando se transfieran datos personales a un tercer país o a una organización internacional, el interesado tendrá derecho a ser informado de las garantías adecuadas en virtud del artículo 46 relativas a la transferencia.

3. El responsable del tratamiento facilitará una copia de los datos personales objeto de tratamiento. El responsable podrá percibir por cualquier otra copia solicitada por el interesado un canon razonable basado en los costes administrativos. Cuando el interesado presente la solicitud por medios electrónicos, y a menos que este solicite que se facilite de otro modo, la información se facilitará en un formato electrónico de uso común.

4. El derecho a obtener copia mencionado en el apartado 3 no afectará negativamente a los derechos y libertades de otros.

Sección 3. Rectificación y supresión

Artículo 16. *Derecho de rectificación.*

El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional.

Artículo 17. *Derecho de supresión («el derecho al olvido»).*

1. El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:

a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;

b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico;

c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2;

d) los datos personales hayan sido tratados ilícitamente;

e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;

f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1.

2. Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.

3. Los apartados 1 y 2 no se aplicarán cuando el tratamiento sea necesario:

a) para ejercer el derecho a la libertad de expresión e información;

b) para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable;

c) por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 9, apartado 2, letras h) e i), y apartado 3;

d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o

e) para la formulación, el ejercicio o la defensa de reclamaciones.

Artículo 18. *Derecho a la limitación del tratamiento.*

1. El interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:

a) el interesado impugne la exactitud de los datos personales en un plazo que permita al responsable verificar la exactitud de los mismos;

b) el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso;

c) el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones;

d) el interesado se haya opuesto al tratamiento en virtud del artículo 21, apartado 1, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

2. Cuando el tratamiento de datos personales se haya limitado en virtud del apartado 1, dichos datos solo podrán ser objeto de tratamiento, con excepción de su conservación, con el consentimiento del interesado o para la formulación, el ejercicio o la defensa de reclamaciones, o con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público importante de la Unión o de un determinado Estado miembro.

3. Todo interesado que haya obtenido la limitación del tratamiento con arreglo al apartado 1 será informado por el responsable antes del levantamiento de dicha limitación.

Artículo 19. *Obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento.*

El responsable del tratamiento comunicará cualquier rectificación o supresión de datos personales o limitación del tratamiento efectuada con arreglo al artículo 16, al artículo 17, apartado 1, y al artículo 18 a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado. El responsable informará al interesado acerca de dichos destinatarios, si este así lo solicita.

Artículo 20. *Derecho a la portabilidad de los datos.*

1. El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando:

a) el tratamiento esté basado en el consentimiento con arreglo al artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), o en un contrato con arreglo al artículo 6, apartado 1, letra b), y
b) el tratamiento se efectúe por medios automatizados.

2. Al ejercer su derecho a la portabilidad de los datos de acuerdo con el apartado 1, el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.
3. El ejercicio del derecho mencionado en el apartado 1 del presente artículo se entenderá sin perjuicio del artículo 17. Tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.
4. El derecho mencionado en el apartado 1 no afectará negativamente a los derechos y libertades de otros.

Sección 4. Derecho de oposición y decisiones individuales automatizadas

Artículo 21. *Derecho de oposición.*

1. El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en lo dispuesto en el artículo 6, apartado 1, letras e) o f), incluida la elaboración de perfiles sobre la base de dichas disposiciones. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.
2. Cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia.
3. Cuando el interesado se oponga al tratamiento con fines de mercadotecnia directa, los datos personales dejarán de ser tratados para dichos fines.
4. A más tardar en el momento de la primera comunicación con el interesado, el derecho indicado en los apartados 1 y 2 será mencionado explícitamente al interesado y será presentado claramente y al margen de cualquier otra información.
5. En el contexto de la utilización de servicios de la sociedad de la información, y no obstante lo dispuesto en la Directiva 2002/58/CE, el interesado podrá ejercer su derecho a oponerse por medios automatizados que apliquen especificaciones técnicas.
6. Cuando los datos personales se traten con fines de investigación científica o histórica o fines estadísticos de conformidad con el artículo 89, apartado 1, el interesado tendrá derecho, por motivos relacionados con su situación particular, a oponerse al tratamiento de datos personales que le conciernan, salvo que sea necesario para el cumplimiento de una misión realizada por razones de interés público.

Artículo 22. *Decisiones individuales automatizadas, incluida la elaboración de perfiles.*

1. Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

2. El apartado 1 no se aplicará si la decisión:

a) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento;

b) está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o

c) se basa en el consentimiento explícito del interesado.

3. En los casos a que se refiere el apartado 2, letras a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.

4. Las decisiones a que se refiere el apartado 2 no se basarán en las categorías especiales de datos personales contempladas en el artículo 9, apartado 1, salvo que se aplique el artículo 9, apartado 2, letra a) o g), y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.

Sección 5. Limitaciones

Artículo 23. *Limitaciones.*

1. El Derecho de la Unión o de los Estados miembros que se aplique al responsable o el encargado del tratamiento podrá limitar, a través de medidas legislativas, el alcance de las obligaciones y de los derechos establecidos en los artículos 12 a 22 y el artículo 34, así como en el artículo 5 en la medida en que sus disposiciones se correspondan con los derechos y obligaciones contemplados en los artículos 12 a 22, cuando tal limitación respete en lo esencial los derechos y libertades fundamentales y sea una medida necesaria y proporcionada en una sociedad democrática para salvaguardar:

a) la seguridad del Estado;

b) la defensa;

c) la seguridad pública;

d) la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención;

e) otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un interés económico o financiero importante de la Unión o de un Estado miembro, inclusive en los ámbitos fiscal, presupuestario y monetario, la sanidad pública y la seguridad social;

f) la protección de la independencia judicial y de los procedimientos judiciales;

g) la prevención, la investigación, la detección y el enjuiciamiento de infracciones de normas deontológicas en las profesiones reguladas;

h) una función de supervisión, inspección o reglamentación vinculada, incluso ocasionalmente, con el ejercicio de la autoridad pública en los casos contemplados en las letras a) a e) y g);

i) la protección del interesado o de los derechos y libertades de otros;

j) la ejecución de demandas civiles.

2. En particular, cualquier medida legislativa indicada en el apartado 1 contendrá como mínimo, en su caso, disposiciones específicas relativas a:

a) la finalidad del tratamiento o de las categorías de tratamiento;

b) las categorías de datos personales de que se trate;

c) el alcance de las limitaciones establecidas;

d) las garantías para evitar accesos o transferencias ilícitos o abusivos;

e) la determinación del responsable o de categorías de responsables;

f) los plazos de conservación y las garantías aplicables habida cuenta de la naturaleza, alcance y objetivos del tratamiento o las categorías de tratamiento;

g) los riesgos para los derechos y libertades de los interesados, y

h) el derecho de los interesados a ser informados sobre la limitación, salvo si puede ser perjudicial a los fines de esta.

CAPÍTULO IV

Responsable del tratamiento y encargado del tratamiento

Sección 1. Obligaciones generales

Artículo 24. *Responsabilidad del responsable del tratamiento.*

1. Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.

2. Cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas en el apartado 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos.

3. La adhesión a códigos de conducta aprobados a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento.

Artículo 25. *Protección de datos desde el diseño y por defecto.*

1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.

2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

3. Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo.

Artículo 26. *Corresponsables del tratamiento.*

1. Cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento serán considerados corresponsables del tratamiento. Los corresponsables determinarán de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por el presente Reglamento, en particular en cuanto al ejercicio de los derechos del interesado y a sus respectivas obligaciones de suministro de información a que se refieren los artículos 13 y 14, salvo, y en la medida en que, sus responsabilidades respectivas se rijan por el Derecho de la Unión o de los Estados

miembros que se les aplique a ellos. Dicho acuerdo podrá designar un punto de contacto para los interesados.

2. El acuerdo indicado en el apartado 1 reflejará debidamente las funciones y relaciones respectivas de los corresponsables en relación con los interesados. Se pondrán a disposición del interesado los aspectos esenciales del acuerdo.

3. Independientemente de los términos del acuerdo a que se refiere el apartado 1, los interesados podrán ejercer los derechos que les reconoce el presente Reglamento frente a, y en contra de, cada uno de los responsables.

Artículo 27. *Representantes de responsables o encargados del tratamiento no establecidos en la Unión.*

1. Cuando sea de aplicación el artículo 3, apartado 2, el responsable o el encargado del tratamiento designará por escrito un representante en la Unión.

2. La obligación establecida en el apartado 1 del presente artículo no será aplicable:

a) al tratamiento que sea ocasional, que no incluyan el manejo a gran escala de categorías especiales de datos indicadas en el artículo 9, apartado 1, o de datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, y que sea improbable que entrañe un riesgo para los derechos y libertades de las personas físicas, teniendo en cuenta la naturaleza, contexto, alcance y objetivos del tratamiento, o

b) a las autoridades u organismos públicos.

3. El representante estará establecido en uno de los Estados miembros en que estén los interesados cuyos datos personales se traten en el contexto de una oferta de bienes o servicios, o cuyo comportamiento esté siendo controlado.

4. El responsable o el encargado del tratamiento encomendará al representante que atienda, junto al responsable o al encargado, o en su lugar, a las consultas, en particular, de las autoridades de control y de los interesados, sobre todos los asuntos relativos al tratamiento, a fin de garantizar el cumplimiento de lo dispuesto en el presente Reglamento.

5. La designación de un representante por el responsable o el encargado del tratamiento se entenderá sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable o encargado.

Artículo 28. *Encargado del tratamiento.*

1. Cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, este elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado.

2. El encargado del tratamiento no recurrirá a otro encargado sin la autorización previa por escrito, específica o general, del responsable. En este último caso, el encargado informará al responsable de cualquier cambio previsto en la incorporación o sustitución de otros encargados, dando así al responsable la oportunidad de oponerse a dichos cambios.

3. El tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. Dicho contrato o acto jurídico estipulará, en particular, que el encargado:

a) tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público;

b) garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza legal;

c) tomará todas las medidas necesarias de conformidad con el artículo 32;

d) respetará las condiciones indicadas en los apartados 2 y 4 para recurrir a otro encargado del tratamiento;

e) asistirá al responsable, teniendo en cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el capítulo III;

f) ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado;

g) a elección del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros;

h) pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.

En relación con lo dispuesto en la letra h) del párrafo primero, el encargado informará inmediatamente al responsable si, en su opinión, una instrucción infringe el presente Reglamento u otras disposiciones en materia de protección de datos de la Unión o de los Estados miembros.

4. Cuando un encargado del tratamiento recurra a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se impondrán a este otro encargado, mediante contrato u otro acto jurídico establecido con arreglo al Derecho de la Unión o de los Estados miembros, las mismas obligaciones de protección de datos que las estipuladas en el contrato u otro acto jurídico entre el responsable y el encargado a que se refiere el apartado 3, en particular la prestación de garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con las disposiciones del presente Reglamento. Si ese otro encargado incumple sus obligaciones de protección de datos, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento por lo que respecta al cumplimiento de las obligaciones del otro encargado.

5. La adhesión del encargado del tratamiento a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá utilizarse como elemento para demostrar la existencia de las garantías suficientes a que se refieren los apartados 1 y 4 del presente artículo.

6. Sin perjuicio de que el responsable y el encargado del tratamiento celebren un contrato individual, el contrato u otro acto jurídico a que se refieren los apartados 3 y 4 del presente artículo podrá basarse, total o parcialmente, en las cláusulas contractuales tipo a que se refieren los apartados 7 y 8 del presente artículo, inclusive cuando formen parte de una certificación concedida al responsable o encargado de conformidad con los artículos 42 y 43.

7. La Comisión podrá fijar cláusulas contractuales tipo para los asuntos a que se refieren los apartados 3 y 4 del presente artículo, de acuerdo con el procedimiento de examen a que se refiere el artículo 93, apartado 2.

8. Una autoridad de control podrá adoptar cláusulas contractuales tipo para los asuntos a que se refieren los apartados 3 y 4 del presente artículo, de acuerdo con el mecanismo de coherencia a que se refiere el artículo 63.

9. El contrato u otro acto jurídico a que se refieren los apartados 3 y 4 constará por escrito, inclusive en formato electrónico.

10. Sin perjuicio de lo dispuesto en los artículos 82, 83 y 84, si un encargado del tratamiento infringe el presente Reglamento al determinar los fines y medios del tratamiento, será considerado responsable del tratamiento con respecto a dicho tratamiento.

Artículo 29. *Tratamiento bajo la autoridad del responsable o del encargado del tratamiento.*

El encargado del tratamiento y cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo podrán tratar dichos datos siguiendo instrucciones del responsable, a no ser que estén obligados a ello en virtud del Derecho de la Unión o de los Estados miembros.

Artículo 30. *Registro de las actividades de tratamiento.*

1. Cada responsable y, en su caso, su representante llevarán un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. Dicho registro deberá contener toda la información indicada a continuación:

a) el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos;
b) los fines del tratamiento;
c) una descripción de las categorías de interesados y de las categorías de datos personales;
d) las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;
e) en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;
f) cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;
g) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 32, apartado 1.

2. Cada encargado y, en su caso, el representante del encargado, llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable que contenga:

a) el nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado, y, en su caso, del representante del responsable o del encargado, y del delegado de protección de datos;
b) las categorías de tratamientos efectuados por cuenta de cada responsable;
c) en su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;
d) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 30, apartado 1.

3. Los registros a que se refieren los apartados 1 y 2 constarán por escrito, inclusive en formato electrónico.
4. El responsable o el encargado del tratamiento y, en su caso, el representante del responsable o del encargado pondrán el registro a disposición de la autoridad de control que lo solicite.
5. Las obligaciones indicadas en los apartados 1 y 2 no se aplicarán a ninguna empresa ni organización que emplee a menos de 250 personas, a menos que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales indicadas en el artículo 9, apartado 1, o datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10.

Artículo 31. *Cooperación con la autoridad de control.*

El responsable y el encargado del tratamiento y, en su caso, sus representantes cooperarán con la autoridad de control que lo solicite en el desempeño de sus funciones.

Sección 2. Seguridad de los datos personales

Artículo 32. *Seguridad del tratamiento.*

1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) la seudonimización y el cifrado de datos personales;
b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.
3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.
4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros.

Artículo 33. *Notificación de una violación de la seguridad de los datos personales a la autoridad de control.*

1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.
2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.
3. La notificación contemplada en el apartado 1 deberá, como mínimo:

a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;
b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;
c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;
d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo.

Artículo 34. *Comunicación de una violación de la seguridad de los datos personales al interesado.*

1. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida.

2. La comunicación al interesado contemplada en el apartado 1 del presente artículo describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 33, apartado 3, letras b), c) y d).

3. La comunicación al interesado a que se refiere el apartado 1 no será necesaria si se cumple alguna de las condiciones siguientes:

a) el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;

b) el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado a que se refiere el apartado 1;

c) suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.

4. Cuando el responsable todavía no haya comunicado al interesado la violación de la seguridad de los datos personales, la autoridad de control, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo haga o podrá decidir que se cumple alguna de las condiciones mencionadas en el apartado 3.

Sección 3. Evaluación de impacto relativa a la protección de datos y consulta previa

Artículo 35. *Evaluación de impacto relativa a la protección de datos.*

1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.

2. El responsable del tratamiento recabará el asesoramiento del delegado de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos.

3. La evaluación de impacto relativa a la protección de los datos a que se refiere el apartado 1 se requerirá en particular en caso de:

a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;

b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o

c) observación sistemática a gran escala de una zona de acceso público.

4. La autoridad de control establecerá y publicará una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos de conformidad con el apartado 1. La autoridad de control comunicará esas listas al Comité a que se refiere el artículo 68.

5. La autoridad de control podrá asimismo establecer y publicar la lista de los tipos de tratamiento que no requieren evaluaciones de impacto relativas a la protección de datos. La autoridad de control comunicará esas listas al Comité.

6. Antes de adoptar las listas a que se refieren los apartados 4 y 5, la autoridad de control competente aplicará el mecanismo de coherencia contemplado en el artículo 63 si esas listas incluyen actividades de tratamiento que guarden relación con la oferta de bienes o servicios a interesados o con la observación del comportamiento de estos en varios Estados miembros, o actividades de tratamiento que puedan afectar sustancialmente a la libre circulación de datos personales en la Unión.

7. La evaluación deberá incluir como mínimo:

a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;

b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;

c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y

d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

8. El cumplimiento de los códigos de conducta aprobados a que se refiere el artículo 40 por los responsables o encargados correspondientes se tendrá debidamente en cuenta al evaluar las repercusiones de las operaciones de tratamiento realizadas por dichos responsables o encargados, en particular a efectos de la evaluación de impacto relativa a la protección de datos.

9. Cuando proceda, el responsable recabará la opinión de los interesados o de sus representantes en relación con el tratamiento previsto, sin perjuicio de la protección de intereses públicos o comerciales o de la seguridad de las operaciones de tratamiento.

10. Cuando el tratamiento de conformidad con el artículo 6, apartado 1, letras c) o e), tenga su base jurídica en el Derecho de la Unión o en el Derecho del Estado miembro que se aplique al responsable del tratamiento, tal Derecho regule la operación específica de tratamiento o conjunto de operaciones en cuestión, y ya se haya realizado una evaluación de impacto relativa a la protección de datos como parte de una evaluación de impacto general en el contexto de la adopción de dicha base jurídica, los apartados 1 a 7 no serán de aplicación excepto si los Estados miembros consideran necesario proceder a dicha evaluación previa a las actividades de tratamiento.

11. En caso necesario, el responsable examinará si el tratamiento es conforme con la evaluación de impacto relativa a la protección de datos, al menos cuando exista un cambio del riesgo que representen las operaciones de tratamiento.

Artículo 36. *Consulta previa.*

1. El responsable consultará a la autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de los datos en virtud del artículo 35 muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para mitigarlo.

2. Cuando la autoridad de control considere que el tratamiento previsto a que se refiere el apartado 1 podría infringir el presente Reglamento, en particular cuando el responsable no

haya identificado o mitigado suficientemente el riesgo, la autoridad de control deberá, en un plazo de ocho semanas desde la solicitud de la consulta, asesorar por escrito al responsable, y en su caso al encargado, y podrá utilizar cualquiera de sus poderes mencionados en el artículo 58. Dicho plazo podrá prorrogarse seis semanas, en función de la complejidad del tratamiento previsto. La autoridad de control informará al responsable y, en su caso, al encargado de tal prórroga en el plazo de un mes a partir de la recepción de la solicitud de consulta, indicando los motivos de la dilación. Estos plazos podrán suspenderse hasta que la autoridad de control haya obtenido la información solicitada a los fines de la consulta.

3. Cuando consulte a la autoridad de control con arreglo al apartado 1, el responsable del tratamiento le facilitará la información siguiente:

a) en su caso, las responsabilidades respectivas del responsable, los corresponsables y los encargados implicados en el tratamiento, en particular en caso de tratamiento dentro de un grupo empresarial;

b) los fines y medios del tratamiento previsto;

c) las medidas y garantías establecidas para proteger los derechos y libertades de los interesados de conformidad con el presente Reglamento;

d) en su caso, los datos de contacto del delegado de protección de datos;

e) la evaluación de impacto relativa a la protección de datos establecida en el artículo 35, y

f) cualquier otra información que solicite la autoridad de control.

4. Los Estados miembros garantizarán que se consulte a la autoridad de control durante la elaboración de toda propuesta de medida legislativa que haya de adoptar un Parlamento nacional, o de una medida reglamentaria basada en dicha medida legislativa, que se refiera al tratamiento.

5. No obstante lo dispuesto en el apartado 1, el Derecho de los Estados miembros podrá obligar a los responsables del tratamiento a consultar a la autoridad de control y a recabar su autorización previa en relación con el tratamiento por un responsable en el ejercicio de una misión realizada en interés público, en particular el tratamiento en relación con la protección social y la salud pública.

Sección 4. Delegado de protección de datos

Artículo 37. *Designación del delegado de protección de datos.*

1. El responsable y el encargado del tratamiento designarán un delegado de protección de datos siempre que:

a) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;

b) las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o

c) las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos con arreglo al artículo 9 o de datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10.

2. Un grupo empresarial podrá nombrar un único delegado de protección de datos siempre que sea fácilmente accesible desde cada establecimiento.

3. Cuando el responsable o el encargado del tratamiento sea una autoridad u organismo público, se podrá designar un único delegado de protección de datos para varias de estas autoridades u organismos, teniendo en cuenta su estructura organizativa y tamaño.

4. En casos distintos de los contemplados en el apartado 1, el responsable o el encargado del tratamiento o las asociaciones y otros organismos que representen a categorías de responsables o encargados podrán designar un delegado de protección de datos o deberán designarlo si así lo exige el Derecho de la Unión o de los Estados miembros. El delegado de protección de datos podrá actuar por cuenta de estas asociaciones y otros organismos que representen a responsables o encargados.

5. El delegado de protección de datos será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39.

6. El delegado de protección de datos podrá formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios.

7. El responsable o el encargado del tratamiento publicarán los datos de contacto del delegado de protección de datos y los comunicarán a la autoridad de control.

Artículo 38. *Posición del delegado de protección de datos.*

1. El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales.

2. El responsable y el encargado del tratamiento respaldarán al delegado de protección de datos en el desempeño de las funciones mencionadas en el artículo 39, facilitando los recursos necesarios para el desempeño de dichas funciones y el acceso a los datos personales y a las operaciones de tratamiento, y para el mantenimiento de sus conocimientos especializados.

3. El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones. No será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones. El delegado de protección de datos rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado.

4. Los interesados podrán ponerse en contacto con el delegado de protección de datos por lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos al amparo del presente Reglamento.

5. El delegado de protección de datos estará obligado a mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones, de conformidad con el Derecho de la Unión o de los Estados miembros.

6. El delegado de protección de datos podrá desempeñar otras funciones y cometidos. El responsable o encargado del tratamiento garantizará que dichas funciones y cometidos no den lugar a conflicto de intereses.

Artículo 39. *Funciones del delegado de protección de datos.*

1. El delegado de protección de datos tendrá como mínimo las siguientes funciones:

a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;

b) supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;

c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35;

d) cooperar con la autoridad de control;

e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.

2. El delegado de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

Sección 5. Códigos de conducta y certificación

Artículo 40. *Códigos de conducta.*

1. Los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán la elaboración de códigos de conducta destinados a contribuir a la correcta aplicación del presente Reglamento, teniendo en cuenta las características específicas de los distintos sectores de tratamiento y las necesidades específicas de las microempresas y las pequeñas y medianas empresas.

2. Las asociaciones y otros organismos representativos de categorías de responsables o encargados del tratamiento podrán elaborar códigos de conducta o modificar o ampliar dichos códigos con objeto de especificar la aplicación del presente Reglamento, como en lo que respecta a:

a) el tratamiento leal y transparente;

b) los intereses legítimos perseguidos por los responsables del tratamiento en contextos específicos;

c) la recogida de datos personales;

d) la seudonimización de datos personales;

e) la información proporcionada al público y a los interesados;

f) el ejercicio de los derechos de los interesados;

g) la información proporcionada a los niños y la protección de estos, así como la manera de obtener el consentimiento de los titulares de la patria potestad o tutela sobre el niño;

h) las medidas y procedimientos a que se refieren los artículos 24 y 25 y las medidas para garantizar la seguridad del tratamiento a que se refiere el artículo 32;

i) la notificación de violaciones de la seguridad de los datos personales a las autoridades de control y la comunicación de dichas violaciones a los interesados;

j) la transferencia de datos personales a terceros países u organizaciones internacionales, o

k) los procedimientos extrajudiciales y otros procedimientos de resolución de conflictos que permitan resolver las controversias entre los responsables del tratamiento y los interesados relativas al tratamiento, sin perjuicio de los derechos de los interesados en virtud de los artículos 77 y 79.

3. Además de la adhesión de los responsables o encargados del tratamiento a los que se aplica el presente Reglamento, los responsables o encargados a los que no se aplica el presente Reglamento en virtud del artículo 3 podrán adherirse también a códigos de conducta aprobados de conformidad con el apartado 5 del presente artículo y que tengan validez general en virtud del apartado 9 del presente artículo, a fin de ofrecer garantías adecuadas en el marco de las transferencias de datos personales a terceros países u organizaciones internacionales a tenor del artículo 46, apartado 2, letra e). Dichos responsables o encargados deberán asumir compromisos vinculantes y exigibles, por vía contractual o mediante otros instrumentos jurídicamente vinculantes, para aplicar dichas garantías adecuadas, incluidas las relativas a los derechos de los interesados.

4. El código de conducta a que se refiere el apartado 2 del presente artículo contendrá mecanismos que permitan al organismo mencionado en el artículo 41, apartado 1, efectuar el control obligatorio del cumplimiento de sus disposiciones por los responsables o encargados de tratamiento que se comprometan a aplicarlo, sin perjuicio de las funciones y los poderes de las autoridades de control que sean competentes con arreglo al artículo 51 o 56.

5. Las asociaciones y otros organismos mencionados en el apartado 2 del presente artículo que proyecten elaborar un código de conducta o modificar o ampliar un código existente presentarán el proyecto de código o la modificación o ampliación a la autoridad de control que sea competente con arreglo al artículo 55. La autoridad de control dictaminará si el proyecto de código o la modificación o ampliación es conforme con el presente Reglamento y aprobará dicho proyecto de código, modificación o ampliación si considera suficientes las garantías adecuadas ofrecidas.

6. Si el proyecto de código o la modificación o ampliación es aprobado de conformidad con el apartado 5 y el código de conducta de que se trate no se refiere a actividades de

tratamiento en varios Estados miembros, la autoridad de control registrará y publicará el código.

7. Si un proyecto de código de conducta guarda relación con actividades de tratamiento en varios Estados miembros, la autoridad de control que sea competente en virtud del artículo 55 lo presentará por el procedimiento mencionado en el artículo 63, antes de su aprobación o de la modificación o ampliación, al Comité, el cual dictaminará si dicho proyecto, modificación o ampliación es conforme con el presente Reglamento o, en la situación indicada en el apartado 3 del presente artículo, ofrece garantías adecuadas.

8. Si el dictamen a que se refiere el apartado 7 confirma que el proyecto de código o la modificación o ampliación cumple lo dispuesto en el presente Reglamento o, en la situación indicada en el apartado 3, ofrece garantías adecuadas, el Comité presentará su dictamen a la Comisión.

9. La Comisión podrá, mediante actos de ejecución, decidir que el código de conducta o la modificación o ampliación aprobados y presentados con arreglo al apartado 8 del presente artículo tengan validez general dentro de la Unión. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.

10. La Comisión dará publicidad adecuada a los códigos aprobados cuya validez general haya sido decidida de conformidad con el apartado 9.

11. El Comité archivará en un registro todos los códigos de conducta, modificaciones y ampliaciones que se aprueben, y los pondrá a disposición pública por cualquier medio apropiado.

Artículo 41. *Supervisión de códigos de conducta aprobados.*

1. Sin perjuicio de las funciones y los poderes de la autoridad de control competente en virtud de los artículos 57 y 58, podrá supervisar el cumplimiento de un código de conducta en virtud del artículo 40 un organismo que tenga el nivel adecuado de pericia en relación con el objeto del código y que haya sido acreditado para tal fin por la autoridad de control competente.

2. El organismo a que se refiere el apartado 1 podrá ser acreditado para supervisar el cumplimiento de un código de conducta si:

a) ha demostrado, a satisfacción de la autoridad de control competente, su independencia y pericia en relación con el objeto del código;

b) ha establecido procedimientos que le permitan evaluar la idoneidad de los responsables y encargados correspondientes para aplicar el código, supervisar el cumplimiento de sus disposiciones y examinar periódicamente su aplicación;

c) ha establecido procedimientos y estructuras para tratar las reclamaciones relativas a infracciones del código o a la manera en que el código haya sido o esté siendo aplicado por un responsable o encargado del tratamiento, y para hacer dichos procedimientos y estructuras transparentes para los interesados y el público, y

d) ha demostrado, a satisfacción de la autoridad de control competente, que sus funciones y cometidos no dan lugar a conflicto de intereses.

3. La autoridad de control competente someterá al Comité, con arreglo al mecanismo de coherencia a que se refiere el artículo 63, el proyecto que fije los requisitos de acreditación de un organismo a que se refiere el apartado 1 del presente artículo.

4. Sin perjuicio de las funciones y los poderes de la autoridad de control competente y de lo dispuesto en el capítulo VIII, un organismo a tenor del apartado 1 del presente artículo deberá, con sujeción a garantías adecuadas, tomar las medidas oportunas en caso de infracción del código por un responsable o encargado del tratamiento, incluida la suspensión o exclusión de este. Informará de dichas medidas y de las razones de las mismas a la autoridad de control competente.

5. La autoridad de control competente revocará la acreditación de un organismo a tenor del apartado 1 si los requisitos de acreditación no se cumplen o han dejado de cumplirse, o si la actuación de dicho organismo infringe el presente Reglamento.

6. El presente artículo no se aplicará al tratamiento realizado por autoridades y organismos públicos.

Artículo 42. *Certificación.*

1. Los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán, en particular a nivel de la Unión, la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos a fin de demostrar el cumplimiento de lo dispuesto en el presente Reglamento en las operaciones de tratamiento de los responsables y los encargados. Se tendrán en cuenta las necesidades específicas de las microempresas y las pequeñas y medianas empresas.

2. Además de la adhesión de los responsables o encargados del tratamiento sujetos al presente Reglamento, podrán establecerse mecanismos de certificación, sellos o marcas de protección de datos aprobados de conformidad con el apartado 5, con objeto de demostrar la existencia de garantías adecuadas ofrecidas por los responsables o encargados no sujetos al presente Reglamento con arreglo al artículo 3 en el marco de transferencias de datos personales a terceros países u organizaciones internacionales a tenor del artículo 46, apartado 2, letra f). Dichos responsables o encargados deberán asumir compromisos vinculantes y exigibles, por vía contractual o mediante otros instrumentos jurídicamente vinculantes, para aplicar dichas garantías adecuadas, incluidas las relativas a los derechos de los interesados.

3. La certificación será voluntaria y estará disponible a través de un proceso transparente.

4. La certificación a que se refiere el presente artículo no limitará la responsabilidad del responsable o encargado del tratamiento en cuanto al cumplimiento del presente Reglamento y se entenderá sin perjuicio de las funciones y los poderes de las autoridades de control que sean competentes en virtud del artículo 55 o 56.

5. La certificación en virtud del presente artículo será expedida por los organismos de certificación a que se refiere el artículo 43 o por la autoridad de control competente, sobre la base de los criterios aprobados por dicha autoridad de conformidad con el artículo 58, apartado 3, o por el Comité de conformidad con el artículo 63. Cuando los criterios sean aprobados por el Comité, esto podrá dar lugar a una certificación común: el Sello Europeo de Protección de Datos.

6. Los responsables o encargados que sometan su tratamiento al mecanismo de certificación dará al organismo de certificación mencionado en el artículo 43, o en su caso a la autoridad de control competente, toda la información y acceso a sus actividades de tratamiento que necesite para llevar a cabo el procedimiento de certificación.

7. La certificación se expedirá a un responsable o encargado de tratamiento por un período máximo de tres años y podrá ser renovada en las mismas condiciones, siempre y cuando se sigan cumpliendo los criterios pertinentes. La certificación será retirada, cuando proceda, por los organismos de certificación a que se refiere el artículo 43, o en su caso por la autoridad de control competente, cuando no se cumplan o se hayan dejado de cumplir los criterios para la certificación.

8. El Comité archivará en un registro todos los mecanismos de certificación y sellos y marcas de protección de datos y los pondrá a disposición pública por cualquier medio apropiado.

Artículo 43. *Organismo de certificación.*

1. Sin perjuicio de las funciones y poderes de la autoridad de control competente en virtud de los artículos 57 y 58, los organismos de certificación que tengan un nivel adecuado de pericia en materia de protección de datos expedirán y renovarán las certificaciones una vez informada la autoridad de control, a fin de esta que pueda ejercer, si así se requiere, sus poderes en virtud del artículo 58, apartado 2, letra h). Los Estados miembros garantizarán que dichos organismos de certificación sean acreditados por la autoridad o el organismo indicado a continuación, o por ambos:

a) la autoridad de control que sea competente en virtud del artículo 55 o 56;

b) el organismo nacional de acreditación designado de conformidad con el Reglamento (CE) n.º 765/2008 del Parlamento Europeo y del Consejo [20] con arreglo a la norma EN ISO/IEC 17065/2012 y a los requisitos adicionales establecidos por la autoridad de control que sea competente en virtud del artículo 55 o 56.

2. Los organismos de certificación mencionados en el apartado 1 únicamente serán acreditados de conformidad con dicho apartado si:

a) han demostrado, a satisfacción de la autoridad de control competente, su independencia y su pericia en relación con el objeto de la certificación;

b) se han comprometido a respetar los criterios mencionados en el artículo 42, apartado 5, y aprobados por la autoridad de control que sea competente en virtud del artículo 55 o 56, o por el Comité de conformidad con el artículo 63;

c) han establecido procedimientos para la expedición, la revisión periódica y la retirada de certificaciones, sellos y marcas de protección de datos;

d) han establecido procedimientos y estructuras para tratar las reclamaciones relativas a infracciones de la certificación o a la manera en que la certificación haya sido o esté siendo aplicada por un responsable o encargado del tratamiento, y para hacer dichos procedimientos y estructuras transparentes para los interesados y el público, y

e) han demostrado, a satisfacción de la autoridad de control competente, que sus funciones y cometidos no dan lugar a conflicto de intereses.

3. La acreditación de los organismos de certificación a que se refieren los apartados 1 y 2 del presente artículo se realizará sobre la base de los requisitos aprobados por la autoridad de control que sea competente en virtud del artículo 55 o 56 o por el Comité en virtud del artículo 63. En caso de acreditación de conformidad con el apartado 1, letra b), del presente artículo, estos requisitos complementarán los contemplados en el Reglamento (CE) n.º 765/2008 y las normas técnicas que describen los métodos y procedimientos de los organismos de certificación.

4. Los organismos de certificación a que se refiere el apartado 1 serán responsable de la correcta evaluación a efectos de certificación o retirada de la certificación, sin perjuicio de la responsabilidad del responsable o del encargado del tratamiento en cuanto al cumplimiento del presente Reglamento. La acreditación se expedirá por un período máximo de cinco años y podrá ser renovada en las mismas condiciones, siempre y cuando el organismo de certificación cumpla los requisitos establecidos en el presente artículo.

5. Los organismos de certificación a que se refiere el apartado 1 comunicarán a las autoridades de control competentes las razones de la expedición de la certificación solicitada o de su retirada.

6. La autoridad de control hará públicos los requisitos a que se refiere el apartado 3 del presente artículo y los criterios a que se refiere el artículo 42, apartado 5, en una forma fácilmente accesible. Las autoridades de control comunicarán también dichos requisitos y criterios al Comité.

7. No obstante lo dispuesto en el capítulo VIII, la autoridad de control competente o el organismo nacional de acreditación revocará la acreditación a un organismo de certificación a tenor del apartado 1 del presente artículo si las condiciones de la acreditación no se cumplen o han dejado de cumplirse, o si la actuación de dicho organismo de certificación infringe el presente Reglamento.

8. La Comisión estará facultada para adoptar actos delegados, de conformidad con el artículo 92, a fin de especificar las condiciones que deberán tenerse en cuenta para los mecanismos de certificación en materia de protección de datos a que se refiere el artículo 42, apartado 1.

9. La Comisión podrá adoptar actos de ejecución que establezcan normas técnicas para los mecanismos de certificación y los sellos y marcas de protección de datos, y mecanismos para promover y reconocer dichos mecanismos de certificación, sellos y marcas. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.

---

[20] Reglamento (CE) n.º 765/2008 del Parlamento Europeo y del Consejo, de 9 de julio de 2008, por el que se establecen los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos y por el que se deroga el Reglamento (CEE) n.º 339/93 (DO L 218 de 13.8.2008, p. 30).

CAPÍTULO V

Transferencias de datos personales a terceros países u organizaciones internacionales

Artículo 44. *Principio general de las transferencias.*

Solo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional si, a reserva de las demás disposiciones del presente Reglamento, el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el presente capítulo, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional. Todas las disposiciones del presente capítulo se aplicarán a fin de asegurar que el nivel de protección de las personas físicas garantizado por el presente Reglamento no se vea menoscabado.

Artículo 45. *Transferencias basadas en una decisión de adecuación.*

1. Podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado. Dicha transferencia no requerirá ninguna autorización específica.

2. Al evaluar la adecuación del nivel de protección, la Comisión tendrá en cuenta, en particular, los siguientes elementos:

a) el Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial, incluida la relativa a la seguridad pública, la defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, las normas de protección de datos, las normas profesionales y las medidas de seguridad, incluidas las normas sobre transferencias ulteriores de datos personales a otro tercer país u organización internacional observadas en ese país u organización internacional, la jurisprudencia, así como el reconocimiento a los interesados cuyos datos personales estén siendo transferidos de derechos efectivos y exigibles y de recursos administrativos y acciones judiciales que sean efectivos;

b) la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las cuales esté sujeta una organización internacional, con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos, incluidos poderes de ejecución adecuados, de asistir y asesorar a los interesados en el ejercicio de sus derechos, y de cooperar con las autoridades de control de la Unión y de los Estados miembros, y

c) los compromisos internacionales asumidos por el tercer país u organización internacional de que se trate, u otras obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes, así como de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales.

3. La Comisión, tras haber evaluado la adecuación del nivel de protección, podrá decidir, mediante un acto de ejecución, que un tercer país, un territorio o uno o varios sectores específicos de un tercer país, o una organización internacional garantizan un nivel de protección adecuado a tenor de lo dispuesto en el apartado 2 del presente artículo. El acto de ejecución establecerá un mecanismo de revisión periódica, al menos cada cuatro años, que tenga en cuenta todos los acontecimientos relevantes en el tercer país o en la organización internacional. El acto de ejecución especificará su ámbito de aplicación territorial y sectorial, y, en su caso, determinará la autoridad o autoridades de control a que se refiere el apartado 2, letra b), del presente artículo. El acto de ejecución se adoptará con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.

4. La Comisión supervisará de manera continuada los acontecimientos en países terceros y organizaciones internacionales que puedan afectar a la efectiva aplicación de las

decisiones adoptadas con arreglo al apartado 3 del presente artículo y de las decisiones adoptadas sobre la base del artículo 25, apartado 6, de la Directiva 95/46/CE.

5. Cuando la información disponible, en particular tras la revisión a que se refiere el apartado 3 del presente artículo, muestre que un tercer país, un territorio o un sector específico de ese tercer país, o una organización internacional ya no garantiza un nivel de protección adecuado a tenor del apartado 2 del presente artículo, la Comisión, mediante actos de ejecución, derogará, modificará o suspenderá, en la medida necesaria y sin efecto retroactivo, la decisión a que se refiere el apartado 3 del presente artículo. Dichos actos de ejecución se adoptarán de acuerdo con el procedimiento de examen a que se refiere el artículo 93, apartado 2.

Por razones imperiosas de urgencia debidamente justificadas, la Comisión adoptará actos de ejecución inmediatamente aplicables de conformidad con el procedimiento a que se refiere el artículo 93, apartado 3.

6 La Comisión entablará consultas con el tercer país u organización internacional con vistas a poner remedio a la situación que dé lugar a la decisión adoptada de conformidad con el apartado 5.

7. Toda decisión de conformidad con el apartado 5 del presente artículo se entenderá sin perjuicio de las transferencias de datos personales al tercer país, a un territorio o uno o varios sectores específicos de ese tercer país, o a la organización internacional de que se trate en virtud de los artículos 46 a 49.

8. La Comisión publicará en el Diario Oficial de la Unión Europea y en su página web una lista de terceros países, territorios y sectores específicos en un tercer país, y organizaciones internacionales respecto de los cuales haya decidido que se garantiza, o ya no, un nivel de protección adecuado.

9. Las decisiones adoptadas por la Comisión en virtud del artículo 25, apartado 6, de la Directiva 95/46/CE permanecerán en vigor hasta que sean modificadas, sustituidas o derogadas por una decisión de la Comisión adoptada de conformidad con los apartados 3 o 5 del presente artículo.

Artículo 46. *Transferencias mediante garantías adecuadas.*

1. A falta de decisión con arreglo al artículo 45, apartado 3, el responsable o el encargado del tratamiento solo podrá transmitir datos personales a un tercer país u organización internacional si hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas.

2. Las garantías adecuadas con arreglo al apartado 1 podrán ser aportadas, sin que se requiera ninguna autorización expresa de una autoridad de control, por:

a) un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos;

b) normas corporativas vinculantes de conformidad con el artículo 47;

c) cláusulas tipo de protección de datos adoptadas por la Comisión de conformidad con el procedimiento de examen a que se refiere el artículo 93, apartado 2;

d) cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión con arreglo al procedimiento de examen a que se refiere en el artículo 93, apartado 2;

e) un código de conducta aprobado con arreglo al artículo 40, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados, o

f) un mecanismo de certificación aprobado con arreglo al artículo 42, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados.

3. Siempre que exista autorización de la autoridad de control competente, las garantías adecuadas contempladas en el apartado 1 podrán igualmente ser aportadas, en particular, mediante:

a) cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional, o

b) disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados.

4. La autoridad de control aplicará el mecanismo de coherencia a que se refiere el artículo 63 en los casos indicados en el apartado 3 del presente artículo.

5. Las autorizaciones otorgadas por un Estado miembro o una autoridad de control de conformidad con el artículo 26, apartado 2, de la Directiva 95/46/CE seguirán siendo válidas hasta que hayan sido modificadas, sustituidas o derogadas, en caso necesario, por dicha autoridad de control. Las decisiones adoptadas por la Comisión en virtud del artículo 26, apartado 4, de la Directiva 95/46/CE permanecerán en vigor hasta que sean modificadas, sustituidas o derogadas, en caso necesario, por una decisión de la Comisión adoptada de conformidad con el apartado 2 del presente artículo.

Artículo 47. *Normas corporativas vinculantes.*

1. La autoridad de control competente aprobará normas corporativas vinculantes de conformidad con el mecanismo de coherencia establecido en el artículo 63, siempre que estas:

a) sean jurídicamente vinculantes y se apliquen y sean cumplidas por todos los miembros correspondientes del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, incluidos sus empleados;

b) confieran expresamente a los interesados derechos exigibles en relación con el tratamiento de sus datos personales, y

c) cumplan los requisitos establecidos en el apartado 2.

2. Las normas corporativas vinculantes mencionadas en el apartado 1 especificarán, como mínimo, los siguientes elementos:

a) la estructura y los datos de contacto del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta y de cada uno de sus miembros;

b) las transferencias o conjuntos de transferencias de datos, incluidas las categorías de datos personales, el tipo de tratamientos y sus fines, el tipo de interesados afectados y el nombre del tercer o los terceros países en cuestión;

c) su carácter jurídicamente vinculante, tanto a nivel interno como externo;

d) la aplicación de los principios generales en materia de protección de datos, en particular la limitación de la finalidad, la minimización de los datos, los periodos de conservación limitados, la calidad de los datos, la protección de los datos desde el diseño y por defecto, la base del tratamiento, el tratamiento de categorías especiales de datos personales, las medidas encaminadas a garantizar la seguridad de los datos y los requisitos con respecto a las transferencias ulteriores a organismos no vinculados por las normas corporativas vinculantes;

e) los derechos de los interesados en relación con el tratamiento y los medios para ejercerlos, en particular el derecho a no ser objeto de decisiones basadas exclusivamente en un tratamiento automatizado, incluida la elaboración de perfiles de conformidad con lo dispuesto en el artículo 22, el derecho a presentar una reclamación ante la autoridad de control competente y ante los tribunales competentes de los Estados miembros de conformidad con el artículo 79, y el derecho a obtener una reparación, y, cuando proceda, una indemnización por violación de las normas corporativas vinculantes;

f) la aceptación por parte del responsable o del encargado del tratamiento establecidos en el territorio de un Estado miembro de la responsabilidad por cualquier violación de las normas corporativas vinculantes por parte de cualquier miembro de que se trate no establecido en la Unión; el responsable o el encargado solo será exonerado, total o parcialmente, de dicha responsabilidad si demuestra que el acto que originó los daños y perjuicios no es imputable a dicho miembro;

g) la forma en que se facilita a los interesados la información sobre las normas corporativas vinculantes, en particular en lo que respecta a las disposiciones contempladas en las letras d), e) y f) del presente apartado, además de los artículos 13 y 14;

h) las funciones de todo delegado de protección de datos designado de conformidad con el artículo 37, o de cualquier otra persona o entidad encargada de la supervisión del cumplimiento de las normas corporativas vinculantes dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, así como de la supervisión de la formación y de la tramitación de las reclamaciones;

i) los procedimientos de reclamación;

j) los mecanismos establecidos dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta para garantizar la verificación del cumplimiento de las normas corporativas vinculantes. Dichos mecanismos incluirán auditorías de protección de datos y métodos para garantizar acciones correctivas para proteger los derechos del interesado. Los resultados de dicha verificación deberían comunicarse a la persona o entidad a que se refiere la letra h) y al consejo de administración de la empresa que controla un grupo empresarial, o de la unión de empresas dedicadas a una actividad económica conjunta, y ponerse a disposición de la autoridad de control competente que lo solicite;

k) los mecanismos establecidos para comunicar y registrar las modificaciones introducidas en las normas y para notificar esas modificaciones a la autoridad de control;

l) el mecanismo de cooperación con la autoridad de control para garantizar el cumplimiento por parte de cualquier miembro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, en particular poniendo a disposición de la autoridad de control los resultados de las verificaciones de las medidas contempladas en la letra j);

m) los mecanismos para informar a la autoridad de control competente de cualquier requisito jurídico de aplicación en un país tercero a un miembro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, que probablemente tengan un efecto adverso sobre las garantías establecidas en las normas corporativas vinculantes, y

n) la formación en protección de datos pertinente para el personal que tenga acceso permanente o habitual a datos personales.

3. La Comisión podrá especificar el formato y los procedimientos para el intercambio de información entre los responsables, los encargados y las autoridades de control en relación con las normas corporativas vinculantes a tenor de lo dispuesto en el presente artículo. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.

Artículo 48. *Transferencias o comunicaciones no autorizadas por el Derecho de la Unión.*

Cualquier sentencia de un órgano jurisdiccional o decisión de una autoridad administrativa de un tercer país que exijan que un responsable o encargado del tratamiento transfiera o comunique datos personales únicamente será reconocida o ejecutable en cualquier modo si se basa en un acuerdo internacional, como un tratado de asistencia jurídica mutua, vigente entre el país tercero requirente y la Unión o un Estado miembro, sin perjuicio de otros motivos para la transferencia al amparo del presente capítulo.

Artículo 49. *Excepciones para situaciones específicas.*

1. En ausencia de una decisión de adecuación de conformidad con el artículo 45, apartado 3, o de garantías adecuadas de conformidad con el artículo 46, incluidas las normas corporativas vinculantes, una transferencia o un conjunto de transferencias de datos personales a un tercer país u organización internacional únicamente se realizará si se cumple alguna de las condiciones siguientes:

a) el interesado haya dado explícitamente su consentimiento a la transferencia propuesta, tras haber sido informado de los posibles riesgos para él de dichas transferencias debido a la ausencia de una decisión de adecuación y de garantías adecuadas;

b) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales adoptadas a solicitud del interesado;

c) la transferencia sea necesaria para la celebración o ejecución de un contrato, en interés del interesado, entre el responsable del tratamiento y otra persona física o jurídica;

d) la transferencia sea necesaria por razones importantes de interés público;

e) la transferencia sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones;

f) la transferencia sea necesaria para proteger los intereses vitales del interesado o de otras personas, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento;

g) la transferencia se realice desde un registro público que, con arreglo al Derecho de la Unión o de los Estados miembros, tenga por objeto facilitar información al público y esté abierto a la consulta del público en general o de cualquier persona que pueda acreditar un interés legítimo, pero sólo en la medida en que se cumplan, en cada caso particular, las condiciones que establece el Derecho de la Unión o de los Estados miembros para la consulta.

Cuando una transferencia no pueda basarse en disposiciones de los artículos 45 o 46, incluidas las disposiciones sobre normas corporativas vinculantes, y no sea aplicable ninguna de las excepciones para situaciones específicas a que se refiere el párrafo primero del presente apartado, solo se podrá llevar a cabo si no es repetitiva, afecta solo a un número limitado de interesados, es necesaria a los fines de intereses legítimos imperiosos perseguidos por el responsable del tratamiento sobre los que no prevalezcan los intereses o derechos y libertades del interesado, y el responsable del tratamiento evaluó todas las circunstancias concurrentes en la transferencia de datos y, basándose en esta evaluación, ofreció garantías apropiadas con respecto a la protección de datos personales. El responsable del tratamiento informará a la autoridad de control de la transferencia. Además de la información a que hacen referencia los artículos 13 y 14, el responsable del tratamiento informará al interesado de la transferencia y de los intereses legítimos imperiosos perseguidos.

2. Una transferencia efectuada de conformidad con el apartado 1, párrafo primero, letra g), no abarcará la totalidad de los datos personales ni categorías enteras de datos personales contenidos en el registro. Si la finalidad del registro es la consulta por parte de personas que tengan un interés legítimo, la transferencia solo se efectuará a solicitud de dichas personas o si estas han de ser las destinatarias.

3. En el apartado 1, el párrafo primero, letras a), b) y c), y el párrafo segundo no serán aplicables a las actividades llevadas a cabo por las autoridades públicas en el ejercicio de sus poderes públicos.

4. El interés público contemplado en el apartado 1, párrafo primero, letra d), será reconocido por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento.

5. En ausencia de una decisión por la que se constate la adecuación de la protección de los datos, el Derecho de la Unión o de los Estados miembros podrá, por razones importantes de interés público, establecer expresamente límites a la transferencia de categorías específicas de datos a un tercer país u organización internacional. Los Estados miembros notificarán a la Comisión dichas disposiciones.

6. El responsable o el encargado del tratamiento documentarán en los registros indicados en el artículo 30 la evaluación y las garantías apropiadas a que se refiere el apartado 1, párrafo segundo, del presente artículo.

Artículo 50. *Cooperación internacional en el ámbito de la protección de datos personales.*

En relación con los terceros países y las organizaciones internacionales, la Comisión y las autoridades de control tomarán medidas apropiadas para:

a) crear mecanismos de cooperación internacional que faciliten la aplicación eficaz de la legislación relativa a la protección de datos personales;

b) prestarse mutuamente asistencia a escala internacional en la aplicación de la legislación relativa a la protección de datos personales, en particular mediante la notificación, la remisión de reclamaciones, la asistencia en las investigaciones y el intercambio de información, a reserva de las garantías adecuadas para la protección de los datos personales y otros derechos y libertades fundamentales;

c) asociar a partes interesadas en la materia a los debates y actividades destinados a reforzar la cooperación internacional en la aplicación de la legislación relativa a la protección de datos personales;

d) promover el intercambio y la documentación de la legislación y las prácticas en materia de protección de datos personales, inclusive en materia de conflictos de jurisdicción con terceros países.

CAPÍTULO VI

Autoridades de control independientes

Sección 1. Independencia

Artículo 51. *Autoridad de control.*

1. Cada Estado miembro establecerá que sea responsabilidad de una o varias autoridades públicas independientes (en adelante «autoridad de control») supervisar la aplicación del presente Reglamento, con el fin de proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento y de facilitar la libre circulación de datos personales en la Unión.

2. Cada autoridad de control contribuirá a la aplicación coherente del presente Reglamento en toda la Unión. A tal fin, las autoridades de control cooperarán entre sí y con la Comisión con arreglo a lo dispuesto en el capítulo VII.

3. Cuando haya varias autoridades de control en un Estado miembro, este designará la autoridad de control que representará a dichas autoridades en el Comité, y establecerá el mecanismo que garantice el cumplimiento por las demás autoridades de las normas relativas al mecanismo de coherencia a que se refiere el artículo 63.

4. Cada Estado miembro notificará a la Comisión las disposiciones legales que adopte de conformidad con el presente capítulo a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier modificación posterior que afecte a dichas disposiciones.

Artículo 52. *Independencia.*

1. Cada autoridad de control actuará con total independencia en el desempeño de sus funciones y en el ejercicio de sus poderes de conformidad con el presente Reglamento.

2. El miembro o los miembros de cada autoridad de control serán ajenos, en el desempeño de sus funciones y en el ejercicio de sus poderes de conformidad con el presente Reglamento, a toda influencia externa, ya sea directa o indirecta, y no solicitarán ni admitirán ninguna instrucción.

3. El miembro o los miembros de cada autoridad de control se abstendrán de cualquier acción que sea incompatible con sus funciones y no participarán, mientras dure su mandato, en ninguna actividad profesional que sea incompatible, remunerada o no.

4. Cada Estado miembro garantizará que cada autoridad de control disponga en todo momento de los recursos humanos, técnicos y financieros, así como de los locales y las infraestructuras necesarios para el cumplimiento efectivo de sus funciones y el ejercicio de sus poderes, incluidos aquellos que haya de ejercer en el marco de la asistencia mutua, la cooperación y la participación en el Comité.

5. Cada Estado miembro garantizará que cada autoridad de control elija y disponga de su propio personal, que estará sujeto a la autoridad exclusiva del miembro o miembros de la autoridad de control interesada.

6. Cada Estado miembro garantizará que cada autoridad de control esté sujeta a un control financiero que no afecte a su independencia y que disponga de un presupuesto anual, público e independiente, que podrá formar parte del presupuesto general del Estado o de otro ámbito nacional.

Artículo 53. *Condiciones generales aplicables a los miembros de la autoridad de control.*

1. Los Estados miembros dispondrán que cada miembro de sus autoridades de control sea nombrado mediante un procedimiento transparente por:

— su Parlamento,
— su Gobierno,
— su Jefe de Estado, o
— un organismo independiente encargado del nombramiento en virtud del Derecho de los Estados miembros.

2. Cada miembro poseerá la titulación, la experiencia y las aptitudes, en particular en el ámbito de la protección de datos personales, necesarias para el cumplimiento de sus funciones y el ejercicio de sus poderes.
3. Los miembros darán por concluidas sus funciones en caso de terminación del mandato, dimisión o jubilación obligatoria, de conformidad con el Derecho del Estado miembro de que se trate.
4. Un miembro será destituido únicamente en caso de conducta irregular grave o si deja de cumplir las condiciones exigidas en el desempeño de sus funciones.

Artículo 54. *Normas relativas al establecimiento de la autoridad de control.*

1. Cada Estado miembro establecerá por ley todos los elementos indicados a continuación:

a) el establecimiento de cada autoridad de control;
b) las cualificaciones y condiciones de idoneidad necesarias para ser nombrado miembro de cada autoridad de control;
c) las normas y los procedimientos para el nombramiento del miembro o miembros de cada autoridad de control;
d) la duración del mandato del miembro o los miembros de cada autoridad de control, no inferior a cuatro años, salvo el primer nombramiento posterior al 24 de mayo de 2016, parte del cual podrá ser más breve cuando sea necesario para proteger la independencia de la autoridad de control por medio de un procedimiento de nombramiento escalonado;
e) el carácter renovable o no del mandato del miembro o los miembros de cada autoridad de control y, en su caso, el número de veces que podrá renovarse;
f) las condiciones por las que se rigen las obligaciones del miembro o los miembros y del personal de cada autoridad de control, las prohibiciones relativas a acciones, ocupaciones y prestaciones incompatibles con el cargo durante el mandato y después del mismo, y las normas que rigen el cese en el empleo.

2. El miembro o miembros y el personal de cada autoridad de control estarán sujetos, de conformidad con el Derecho de la Unión o de los Estados miembros, al deber de secreto profesional, tanto durante su mandato como después del mismo, con relación a las informaciones confidenciales de las que hayan tenido conocimiento en el cumplimiento de sus funciones o el ejercicio de sus poderes. Durante su mandato, dicho deber de secreto profesional se aplicará en particular a la información recibida de personas físicas en relación con infracciones del presente Reglamento.

Sección 2. Competencia, funciones y poderes

Artículo 55. *Competencia.*

1. Cada autoridad de control será competente para desempeñar las funciones que se le asignen y ejercer los poderes que se le confieran de conformidad con el presente Reglamento en el territorio de su Estado miembro.
2. Cuando el tratamiento sea efectuado por autoridades públicas o por organismos privados que actúen con arreglo al artículo 6, apartado 1, letras c) o e), será competente la autoridad de control del Estado miembro de que se trate. No será aplicable en tales casos el artículo 56.

3. Las autoridades de control no serán competentes para controlar las operaciones de tratamiento efectuadas por los tribunales en el ejercicio de su función judicial.

Artículo 56. *Competencia de la autoridad de control principal.*

1. Sin perjuicio de lo dispuesto en el artículo 55, la autoridad de control del establecimiento principal o del único establecimiento del responsable o del encargado del tratamiento será competente para actuar como autoridad de control principal para el tratamiento transfronterizo realizado por parte de dicho responsable o encargado con arreglo al procedimiento establecido en el artículo 60.

2. No obstante lo dispuesto en el apartado 1, cada autoridad de control será competente para tratar una reclamación que le sea presentada o una posible infracción del presente Reglamento, en caso de que se refiera únicamente a un establecimiento situado en su Estado miembro o únicamente afecte de manera sustancial a interesados en su Estado miembro.

3. En los casos a que se refiere el apartado 2 del presente artículo, la autoridad de control informará sin dilación al respecto a la autoridad de control principal. En el plazo de tres semanas después de haber sido informada, la autoridad de control principal decidirá si tratará o no el caso de conformidad con el procedimiento establecido en el artículo 60, teniendo presente si existe un establecimiento del responsable o encargado del tratamiento en el Estado miembro de la autoridad de control que le haya informado.

4. En caso de que la autoridad de control principal decida tratar el caso, se aplicará el procedimiento establecido en el artículo 60. La autoridad de control que haya informado a la autoridad de control principal podrá presentarle un proyecto de decisión. La autoridad de control principal tendrá en cuenta en la mayor medida posible dicho proyecto al preparar el proyecto de decisión a que se refiere el artículo 60, apartado 3.

5. En caso de que la autoridad de control principal decida no tratar el caso, la autoridad de control que le haya informado lo tratará con arreglo a los artículos 61 y 62.

6. La autoridad de control principal será el único interlocutor del responsable o del encargado en relación con el tratamiento transfronterizo realizado por dicho responsable o encargado.

Artículo 57. *Funciones.*

1. Sin perjuicio de otras funciones en virtud del presente Reglamento, incumbirá a cada autoridad de control, en su territorio:

a) controlar la aplicación del presente Reglamento y hacerlo aplicar;

b) promover la sensibilización del público y su comprensión de los riesgos, normas, garantías y derechos en relación con el tratamiento. Las actividades dirigidas específicamente a los niños deberán ser objeto de especial atención;

c) asesorar, con arreglo al Derecho de los Estados miembros, al Parlamento nacional, al Gobierno y a otras instituciones y organismos sobre las medidas legislativas y administrativas relativas a la protección de los derechos y libertades de las personas físicas con respecto al tratamiento;

d) promover la sensibilización de los responsables y encargados del tratamiento acerca de las obligaciones que les incumben en virtud del presente Reglamento;

e) previa solicitud, facilitar información a cualquier interesado en relación con el ejercicio de sus derechos en virtud del presente Reglamento y, en su caso, cooperar a tal fin con las autoridades de control de otros Estados miembros;

f) tratar las reclamaciones presentadas por un interesado o por un organismo, organización o asociación de conformidad con el artículo 80, e investigar, en la medida oportuna, el motivo de la reclamación e informar al reclamante sobre el curso y el resultado de la investigación en un plazo razonable, en particular si fueran necesarias nuevas investigaciones o una coordinación más estrecha con otra autoridad de control;

g) cooperar, en particular compartiendo información, con otras autoridades de control y prestar asistencia mutua con el fin de garantizar la coherencia en la aplicación y ejecución del presente Reglamento;

h) llevar a cabo investigaciones sobre la aplicación del presente Reglamento, en particular basándose en información recibida de otra autoridad de control u otra autoridad pública;

i) hacer un seguimiento de cambios que sean de interés, en la medida en que tengan incidencia en la protección de datos personales, en particular el desarrollo de las tecnologías de la información y la comunicación y las prácticas comerciales;

j) adoptar las cláusulas contractuales tipo a que se refieren el artículo 28, apartado 8, y el artículo 46, apartado 2, letra d);

k) elaborar y mantener una lista relativa al requisito de la evaluación de impacto relativa a la protección de datos, en virtud del artículo 35, apartado 4;

l) ofrecer asesoramiento sobre las operaciones de tratamiento contempladas en el artículo 36, apartado 2;

m) alentar la elaboración de códigos de conducta con arreglo al artículo 40, apartado 1, y dictaminar y aprobar los códigos de conducta que den suficientes garantías con arreglo al artículo 40, apartado 5;

n) fomentar la creación de mecanismos de certificación de la protección de datos y de sellos y marcas de protección de datos con arreglo al artículo 42, apartado 1, y aprobar los criterios de certificación de conformidad con el artículo 42, apartado 5;

o) llevar a cabo, si procede, una revisión periódica de las certificaciones expedidas en virtud del artículo 42, apartado 7;

p) elaborar y publicar los requisitos para la acreditación de organismos de supervisión de los códigos de conducta con arreglo al artículo 41 y de organismos de certificación con arreglo al artículo 43;

q) efectuar la acreditación de organismos de supervisión de los códigos de conducta con arreglo al artículo 41 y de organismos de certificación con arreglo al artículo 43;

r) autorizar las cláusulas contractuales y disposiciones a que se refiere el artículo 46, apartado 3;

s) aprobar normas corporativas vinculantes de conformidad con lo dispuesto en el artículo 47;

t) contribuir a las actividades del Comité;

u) llevar registros internos de las infracciones del presente Reglamento y de las medidas adoptadas de conformidad con el artículo 58, apartado 2, y

v) desempeñar cualquier otra función relacionada con la protección de los datos personales.

2. Cada autoridad de control facilitará la presentación de las reclamaciones contempladas en el apartado 1, letra f), mediante medidas como un formulario de presentación de reclamaciones que pueda cumplimentarse también por medios electrónicos, sin excluir otros medios de comunicación.

3. El desempeño de las funciones de cada autoridad de control será gratuito para el interesado y, en su caso, para el delegado de protección de datos.

4. Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, la autoridad de control podrá establecer una tasa razonable basada en los costes administrativos o negarse a actuar respecto de la solicitud. La carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud recaerá en la autoridad de control.

Artículo 58. *Poderes.*

1. Cada autoridad de control dispondrá de todos los poderes de investigación indicados a continuación:

a) ordenar al responsable y al encargado del tratamiento y, en su caso, al representante del responsable o del encargado, que faciliten cualquier información que requiera para el desempeño de sus funciones;

b) llevar a cabo investigaciones en forma de auditorías de protección de datos;

c) llevar a cabo una revisión de las certificaciones expedidas en virtud del artículo 42, apartado 7;

d) notificar al responsable o al encargado del tratamiento las presuntas infracciones del presente Reglamento;

e) obtener del responsable y del encargado del tratamiento el acceso a todos los datos personales y a toda la información necesaria para el ejercicio de sus funciones;

f) obtener el acceso a todos los locales del responsable y del encargado del tratamiento, incluidos cualesquiera equipos y medios de tratamiento de datos, de conformidad con el Derecho procesal de la Unión o de los Estados miembros.

2. Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:

a) dirigir a todo responsable o encargado del tratamiento una advertencia cuando las operaciones de tratamiento previstas puedan infringir lo dispuesto en el presente Reglamento;

b) dirigir a todo responsable o encargado del tratamiento un apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento;

c) ordenar al responsable o encargado del tratamiento que atiendan las solicitudes de ejercicio de los derechos del interesado en virtud del presente Reglamento;

d) ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado;

e) ordenar al responsable del tratamiento que comunique al interesado las violaciones de la seguridad de los datos personales;

f) imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición;

g) ordenar la rectificación o supresión de datos personales o la limitación de tratamiento con arreglo a los artículos 16, 17 y 18 y la notificación de dichas medidas a los destinatarios a quienes se hayan comunicado datos personales con arreglo a al artículo 17, apartado 2, y al artículo 19;

h) retirar una certificación u ordenar al organismo de certificación que retire una certificación emitida con arreglo a los artículos 42 y 43, u ordenar al organismo de certificación que no se emita una certificación si no se cumplen o dejan de cumplirse los requisitos para la certificación;

i) imponer una multa administrativa con arreglo al artículo 83, además o en lugar de las medidas mencionadas en el presente apartado, según las circunstancias de cada caso particular;

j) ordenar la suspensión de los flujos de datos hacia un destinatario situado en un tercer país o hacia una organización internacional.

3. Cada autoridad de control dispondrá de todos los poderes de autorización y consultivos indicados a continuación:

a) asesorar al responsable del tratamiento conforme al procedimiento de consulta previa contemplado en el artículo 36;

b) emitir, por iniciativa propia o previa solicitud, dictámenes destinados al Parlamento nacional, al Gobierno del Estado miembro o, con arreglo al Derecho de los Estados miembros, a otras instituciones y organismos, así como al público, sobre cualquier asunto relacionado con la protección de los datos personales;

c) autorizar el tratamiento a que se refiere el artículo 36, apartado 5, si el Derecho del Estado miembro requiere tal autorización previa;

d) emitir un dictamen y aprobar proyectos de códigos de conducta de conformidad con lo dispuesto en el artículo 40, apartado 5;

e) acreditar los organismos de certificación con arreglo al artículo 43;

f) expedir certificaciones y aprobar criterios de certificación con arreglo al artículo 42, apartado 5;

g) adoptar las cláusulas tipo de protección de datos contempladas en el artículo 28, apartado 8, y el artículo 46, apartado 2, letra d);

h) autorizar las cláusulas contractuales indicadas en el artículo 46, apartado 3, letra a);

i) autorizar los acuerdos administrativos contemplados en el artículo 46, apartado 3, letra b);

j) aprobar normas corporativas vinculantes de conformidad con lo dispuesto en el artículo 47.

4. El ejercicio de los poderes conferidos a la autoridad de control en virtud del presente artículo estará sujeto a las garantías adecuadas, incluida la tutela judicial efectiva y al respeto de las garantías procesales, establecidas en el Derecho de la Unión y de los Estados miembros de conformidad con la Carta.

5. Cada Estado miembro dispondrá por ley que su autoridad de control esté facultada para poner en conocimiento de las autoridades judiciales las infracciones del presente Reglamento y, si procede, para iniciar o ejercitar de otro modo acciones judiciales, con el fin de hacer cumplir lo dispuesto en el mismo.

6. Cada Estado miembro podrá establecer por ley que su autoridad de control tenga otros poderes además de los indicadas en los apartados 1, 2 y 3. El ejercicio de dichos poderes no será obstáculo a la aplicación efectiva del capítulo VII.

Artículo 59. *Informe de actividad.*

Cada autoridad de control elaborará un informe anual de sus actividades, que podrá incluir una lista de tipos de infracciones notificadas y de tipos de medidas adoptadas de conformidad con el artículo 58, apartado 2. Los informes se transmitirán al Parlamento nacional, al Gobierno y a las demás autoridades designadas en virtud del Derecho de los Estados miembros. Se pondrán a disposición del público, de la Comisión y del Comité.

CAPÍTULO VII

Cooperación y coherencia

Sección 1. Cooperación y coherencia

Artículo 60. *Cooperación entre la autoridad de control principal y las demás autoridades de control interesadas.*

1. La autoridad de control principal cooperará con las demás autoridades de control interesadas de acuerdo con el presente artículo, esforzándose por llegar a un consenso. La autoridad de control principal y las autoridades de control interesadas se intercambiarán toda información pertinente.

2. La autoridad de control principal podrá solicitar en cualquier momento a otras autoridades de control interesadas que presten asistencia mutua con arreglo al artículo 61, y podrá llevar a cabo operaciones conjuntas con arreglo al artículo 62, en particular para realizar investigaciones o supervisar la aplicación de una medida relativa a un responsable o un encargado del tratamiento establecido en otro Estado miembro.

3. La autoridad de control principal comunicará sin dilación a las demás autoridades de control interesadas la información pertinente a este respecto. Transmitirá sin dilación un proyecto de decisión a las demás autoridades de control interesadas para obtener su dictamen al respecto y tendrá debidamente en cuenta sus puntos de vista.

4. En caso de que cualquiera de las autoridades de control interesadas formule una objeción pertinente y motivada acerca del proyecto de decisión en un plazo de cuatro semanas a partir de la consulta con arreglo al apartado 3 del presente artículo, la autoridad de control principal someterá el asunto, en caso de que no siga lo indicado en la objeción pertinente y motivada o estime que dicha objeción no es pertinente o no está motivada, al mecanismo de coherencia contemplado en el artículo 63.

5. En caso de que la autoridad de control principal prevea seguir lo indicado en la objeción pertinente y motivada recibida, presentará a dictamen de las demás autoridades de control interesadas un proyecto de decisión revisado. Dicho proyecto de decisión revisado se someterá al procedimiento indicado en el apartado 4 en un plazo de dos semanas.

6. En caso de que ninguna otra autoridad de control interesada haya presentado objeciones al proyecto de decisión transmitido por la autoridad de control principal en el plazo indicado en los apartados 4 y 5, se considerará que la autoridad de control principal y

las autoridades de control interesadas están de acuerdo con dicho proyecto de decisión y estarán vinculadas por este.

7. La autoridad de control principal adoptará y notificará la decisión al establecimiento principal o al establecimiento único del responsable o el encargado del tratamiento, según proceda, e informará de la decisión a las autoridades de control interesadas y al Comité, incluyendo un resumen de los hechos pertinentes y la motivación. La autoridad de control ante la que se haya presentado una reclamación informará de la decisión al reclamante.

8. No obstante lo dispuesto en el apartado 7, cuando se desestime o rechace una reclamación, la autoridad de control ante la que se haya presentado adoptará la decisión, la notificará al reclamante e informará de ello al responsable del tratamiento.

9. En caso de que la autoridad de control principal y las autoridades de control interesadas acuerden desestimar o rechazar determinadas partes de una reclamación y atender otras partes de ella, se adoptará una decisión separada para cada una de esas partes del asunto. La autoridad de control principal adoptará la decisión respecto de la parte referida a acciones en relación con el responsable del tratamiento, la notificará al establecimiento principal o al único establecimiento del responsable o del encargado en el territorio de su Estado miembro, e informará de ello al reclamante, mientras que la autoridad de control del reclamante adoptará la decisión respecto de la parte relativa a la desestimación o rechazo de dicha reclamación, la notificará a dicho reclamante e informará de ello al responsable o al encargado.

10. Tras recibir la notificación de la decisión de la autoridad de control principal con arreglo a los apartados 7 y 9, el responsable o el encargado del tratamiento adoptará las medidas necesarias para garantizar el cumplimiento de la decisión en lo tocante a las actividades de tratamiento en el contexto de todos sus establecimientos en la Unión. El responsable o el encargado notificarán las medidas adoptadas para dar cumplimiento a dicha decisión a la autoridad de control principal, que a su vez informará a las autoridades de control interesadas.

11. En circunstancias excepcionales, cuando una autoridad de control interesada tenga motivos para considerar que es urgente intervenir para proteger los intereses de los interesados, se aplicará el procedimiento de urgencia a que se refiere el artículo 66.

12. La autoridad de control principal y las demás autoridades de control interesadas se facilitarán recíprocamente la información requerida en el marco del presente artículo por medios electrónicos, utilizando un formulario normalizado.

Artículo 61. *Asistencia mutua.*

1. Las autoridades de control se facilitarán información útil y se prestarán asistencia mutua a fin de aplicar el presente Reglamento de manera coherente, y tomarán medidas para asegurar una efectiva cooperación entre ellas. La asistencia mutua abarcará, en particular, las solicitudes de información y las medidas de control, como las solicitudes para llevar a cabo autorizaciones y consultas previas, inspecciones e investigaciones.

2. Cada autoridad de control adoptará todas las medidas oportunas requeridas para responder a una solicitud de otra autoridad de control sin dilación indebida y a más tardar en el plazo de un mes a partir de la solicitud. Dichas medidas podrán incluir, en particular, la transmisión de información pertinente sobre el desarrollo de una investigación.

3. Las solicitudes de asistencia deberán contener toda la información necesaria, entre otras cosas respecto de la finalidad y los motivos de la solicitud. La información que se intercambie se utilizará únicamente para el fin para el que haya sido solicitada.

4. La autoridad de control requerida no podrá negarse a responder a una solicitud, salvo si:

a) no es competente en relación con el objeto de la solicitud o con las medidas cuya ejecución se solicita, o

b) el hecho de responder a la solicitud infringiría el presente Reglamento o el Derecho de la Unión o de los Estados miembros que se aplique a la autoridad de control a la que se dirigió la solicitud.

5. La autoridad de control requerida informará a la autoridad de control requirente de los resultados obtenidos o, en su caso, de los progresos registrados o de las medidas

adoptadas para responder a su solicitud. La autoridad de control requerida explicará los motivos de su negativa a responder a una solicitud al amparo del apartado 4.

6. Como norma general, las autoridades de control requeridas facilitarán la información solicitada por otras autoridades de control por medios electrónicos, utilizando un formato normalizado.

7. Las autoridades de control requeridas no cobrarán tasa alguna por las medidas adoptadas a raíz de una solicitud de asistencia mutua. Las autoridades de control podrán convenir normas de indemnización recíproca por gastos específicos derivados de la prestación de asistencia mutua en circunstancias excepcionales.

8. Cuando una autoridad de control no facilite la información mencionada en el apartado 5 del presente artículo en el plazo de un mes a partir de la recepción de la solicitud de otra autoridad de control, la autoridad de control requirente podrá adoptar una medida provisional en el territorio de su Estado miembro de conformidad con lo dispuesto en el artículo 55, apartado 1. En ese caso, se supondrá que existe la necesidad urgente contemplada en el artículo 66, apartado 1, que exige una decisión urgente y vinculante del Comité en virtud del artículo 66, apartado 2.

9. La Comisión podrá, mediante actos de ejecución, especificar el formato y los procedimientos de asistencia mutua contemplados en el presente artículo, así como las modalidades del intercambio de información por medios electrónicos entre las autoridades de control y entre las autoridades de control y el Comité, en especial el formato normalizado mencionado en el apartado 6 del presente artículo. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.

Artículo 62. *Operaciones conjuntas de las autoridades de control.*

1. Las autoridades de control realizarán, en su caso, operaciones conjuntas, incluidas investigaciones conjuntas y medidas de ejecución conjuntas, en las que participen miembros o personal de las autoridades de control de otros Estados miembros.

2. Si el responsable o el encargado del tratamiento tiene establecimientos en varios Estados miembros o si es probable que un número significativo de interesados en más de un Estado miembro se vean sustancialmente afectados por las operaciones de tratamiento, una autoridad de control de cada uno de esos Estados miembros tendrá derecho a participar en operaciones conjuntas. La autoridad de control que sea competente en virtud del artículo 56, apartados 1 o 4, invitará a la autoridad de control de cada uno de dichos Estados miembros a participar en las operaciones conjuntas y responderá sin dilación a la solicitud de participación presentada por una autoridad de control.

3. Una autoridad de control podrá, con arreglo al Derecho de su Estado miembro y con la autorización de la autoridad de control de origen, conferir poderes, incluidos poderes de investigación, a los miembros o al personal de la autoridad de control de origen que participen en operaciones conjuntas, o aceptar, en la medida en que lo permita el Derecho del Estado miembro de la autoridad de control de acogida, que los miembros o el personal de la autoridad de control de origen ejerzan sus poderes de investigación de conformidad con el Derecho del Estado miembro de la autoridad de control de origen. Dichos poderes de investigación solo podrán ejercerse bajo la orientación y en presencia de miembros o personal de la autoridad de control de acogida. Los miembros o el personal de la autoridad de control de origen estarán sujetos al Derecho del Estado miembro de la autoridad de control de acogida.

4. Cuando participe, de conformidad con el apartado 1, personal de la autoridad de control de origen en operaciones en otro Estado miembro, el Estado miembro de la autoridad de control de acogida asumirá la responsabilidad de acuerdo con el Derecho del Estado miembro en cuyo territorio se desarrollen las operaciones, por los daños y perjuicios que haya causado dicho personal en el transcurso de las mismas.

5. El Estado miembro en cuyo territorio se causaron los daños y perjuicios asumirá su reparación en las condiciones aplicables a los daños y perjuicios causados por su propio personal. El Estado miembro de la autoridad de control de origen cuyo personal haya causado daños y perjuicios a cualquier persona en el territorio de otro Estado miembro le restituirá íntegramente los importes que este último haya abonado a los derechohabientes.

6. Sin perjuicio del ejercicio de sus derechos frente a terceros y habida cuenta de la excepción establecida en el apartado 5, los Estados miembros renunciarán, en el caso contemplado en el apartado 1, a solicitar de otro Estado miembro el reembolso del importe de los daños y perjuicios mencionados en el apartado 4.

7. Cuando se prevea una operación conjunta y una autoridad de control no cumpla en el plazo de un mes con la obligación establecida en el apartado 2, segunda frase, del presente artículo, las demás autoridades de control podrán adoptar una medida provisional en el territorio de su Estado miembro de conformidad con el artículo 55. En ese caso, se presumirá la existencia de una necesidad urgente a tenor del artículo 66, apartado 1, y se requerirá dictamen o decisión vinculante urgente del Comité en virtud del artículo 66, apartado 2.

Sección 2. Coherencia

Artículo 63. *Mecanismo de coherencia.*

A fin de contribuir a la aplicación coherente del presente Reglamento en toda la Unión, las autoridades de control cooperarán entre sí y, en su caso, con la Comisión, en el marco del mecanismo de coherencia establecido en la presente sección.

Artículo 64. *Dictamen del Comité.*

1. El Comité emitirá un dictamen siempre que una autoridad de control competente proyecte adoptar alguna de las medidas enumeradas a continuación. A tal fin, la autoridad de control competente comunicará el proyecto de decisión al Comité, cuando la decisión:

a) tenga por objeto adoptar una lista de las operaciones de tratamiento supeditadas al requisito de la evaluación de impacto relativa a la protección de datos de conformidad con el artículo 35, apartado 4;

b) afecte a un asunto de conformidad con el artículo 40, apartado 7, cuyo objeto sea determinar si un proyecto de código de conducta o una modificación o ampliación de un código de conducta es conforme con el presente Reglamento;

c) tenga por objeto aprobar los requisitos para la acreditación de un organismo con arreglo al artículo 41, apartado 3, de un organismo de certificación conforme al artículo 43, apartado 3, o los criterios aplicables a la certificación a que se refiere el artículo 42, apartado 5;

d) tenga por objeto determinar las cláusulas tipo de protección de datos contempladas en el artículo 46, apartado 2, letra d), y el artículo 28, apartado 8;

e) tenga por objeto autorizar las cláusulas contractuales a que se refiere el artículo 46, apartado 3, letra a);

f) tenga por objeto la aprobación de normas corporativas vinculantes a tenor del artículo 47.

2. Cualquier autoridad de control, el presidente del Comité o la Comisión podrán solicitar que cualquier asunto de aplicación general o que surta efecto en más de un Estado miembro sea examinado por el Comité a efectos de dictamen, en particular cuando una autoridad de control competente incumpla las obligaciones relativas a la asistencia mutua con arreglo al artículo 61 o las operaciones conjuntas con arreglo al artículo 62.

3. En los casos a que se refieren los apartados 1 y 2, el Comité emitirá dictamen sobre el asunto que le haya sido presentado siempre que no haya emitido ya un dictamen sobre el mismo asunto. Dicho dictamen se adoptará en el plazo de ocho semanas por mayoría simple de los miembros del Comité. Dicho plazo podrá prorrogarse seis semanas más, teniendo en cuenta la complejidad del asunto. Por lo que respecta al proyecto de decisión a que se refiere el apartado 1 y distribuido a los miembros del Comité con arreglo al apartado 5, todo miembro que no haya presentado objeciones dentro de un plazo razonable indicado por el presidente se considerará conforme con el proyecto de decisión.

4. Las autoridades de control y la Comisión comunicarán sin dilación por vía electrónica al Comité, utilizando un formato normalizado, toda información útil, en particular, cuando proceda, un resumen de los hechos, el proyecto de decisión, los motivos por los que es necesaria tal medida, y las opiniones de otras autoridades de control interesadas.

5. La Presidencia del Comité informará sin dilación indebida por medios electrónicos:

a) a los miembros del Comité y a la Comisión de cualquier información pertinente que le haya sido comunicada, utilizando un formato normalizado. La secretaría del Comité facilitará, de ser necesario, traducciones de la información que sea pertinente, y

b) a la autoridad de control contemplada, en su caso, en los apartados 1 y 2 y a la Comisión del dictamen, y lo publicará.

6. La autoridad de control competente a que se refiere el apartado 1 no adoptará su proyecto de decisión a tenor del apartado 1 en el plazo mencionado en el apartado 3.

7. La autoridad de control competente a que se refiere el apartado 1 tendrá en cuenta en la mayor medida posible el dictamen del Comité y, en el plazo de dos semanas desde la recepción del dictamen, comunicará por medios electrónicos al presidente del Comité si va a mantener o modificar su proyecto de decisión y, si lo hubiera, el proyecto de decisión modificado, utilizando un formato normalizado.

8. Cuando la autoridad de control competente a que se refiere el apartado 1 informe al presidente del Comité, en el plazo mencionado en el apartado 7 del presente artículo, de que no prevé seguir el dictamen del Comité, en todo o en parte, alegando los motivos correspondientes, se aplicará el artículo 65, apartado 1.

Artículo 65. *Resolución de conflictos por el Comité.*

1. Con el fin de garantizar una aplicación correcta y coherente del presente Reglamento en casos concretos, el Comité adoptará una decisión vinculante en los siguientes casos:

a) cuando, en un caso mencionado en el artículo 60, apartado 4, una autoridad de control interesada haya manifestado una objeción pertinente y motivada a un proyecto de decisión de la autoridad de control principal y esta no haya seguido la objeción o haya rechazado dicha objeción por no ser pertinente o no estar motivada. La decisión vinculante afectará a todos los asuntos a que se refiera la objeción pertinente y motivada, en particular si hay infracción del presente Reglamento;

b) cuando haya puntos de vista enfrentados sobre cuál de las autoridades de control interesadas es competente para el establecimiento principal;

c) cuando una autoridad de control competente no solicite dictamen al Comité en los casos contemplados en el artículo 64, apartado 1, o no siga el dictamen del Comité emitido en virtud del artículo 64. En tal caso, cualquier autoridad de control interesada, o la Comisión, lo pondrá en conocimiento del Comité.

2. La decisión a que se refiere el apartado 1 se adoptará en el plazo de un mes a partir de la remisión del asunto, por mayoría de dos tercios de los miembros del Comité. Este plazo podrá prorrogarse un mes más, habida cuenta de la complejidad del asunto. La decisión que menciona el apartado 1 estará motivada y será dirigida a la autoridad de control principal y a todas las autoridades de control interesadas, y será vinculante para ellas.

3. Cuando el Comité no haya podido adoptar una decisión en los plazos mencionados en el apartado 2, adoptará su decisión en un plazo de dos semanas tras la expiración del segundo mes a que se refiere el apartado 2, por mayoría simple de sus miembros. En caso de empate, decidirá el voto del presidente.

4. Las autoridades de control interesadas no adoptarán decisión alguna sobre el asunto presentado al Comité en virtud del apartado 1 durante los plazos de tiempo a que se refieren los apartados 2 y 3.

5. El presidente del Comité notificará sin dilación indebida la decisión contemplada en el apartado 1 a las autoridades de control interesadas. También informará de ello a la Comisión. La decisión se publicará en el sitio web del Comité sin demora, una vez que la autoridad de control haya notificado la decisión definitiva a que se refiere el apartado 6.

6. La autoridad de control principal o, en su caso, la autoridad de control ante la que se presentó la reclamación adoptará su decisión definitiva sobre la base de la decisión contemplada en el apartado 1 del presente artículo, sin dilación indebida y a más tardar un mes tras la notificación de la decisión del Comité. La autoridad de control principal o, en su caso, la autoridad de control ante la que se presentó la reclamación informará al Comité de la fecha de notificación de su decisión definitiva al responsable o al encargado del

tratamiento y al interesado, respectivamente. La decisión definitiva de las autoridades de control interesadas será adoptada en los términos establecidos en el artículo 60, apartados 7, 8 y 9. La decisión definitiva hará referencia a la decisión contemplada en el apartado 1 del presente artículo y especificará que esta última decisión se publicará en el sitio web del Comité con arreglo al apartado 5 del presente artículo. La decisión definitiva llevará adjunta la decisión contemplada en el apartado 1 del presente artículo.

Artículo 66. *Procedimiento de urgencia.*

1. En circunstancias excepcionales, cuando una autoridad de control interesada considere que es urgente intervenir para proteger los derechos y las libertades de interesados, podrá, como excepción al mecanismo de coherencia contemplado en los artículos 63, 64 y 65, o al procedimiento mencionado en el artículo 60, adoptar inmediatamente medidas provisionales destinadas a producir efectos jurídicos en su propio territorio, con un periodo de validez determinado que no podrá ser superior a tres meses. La autoridad de control comunicará sin dilación dichas medidas, junto con los motivos de su adopción, a las demás autoridades de control interesadas, al Comité y a la Comisión.

2. Cuando una autoridad de control haya adoptado una medida de conformidad con el apartado 1, y considere que deben adoptarse urgentemente medidas definitivas, podrá solicitar con carácter urgente un dictamen o una decisión vinculante urgente del Comité, motivando dicha solicitud de dictamen o decisión.

3. Cualquier autoridad de control podrá solicitar, motivando su solicitud, y, en particular, la urgencia de la intervención, un dictamen urgente o una decisión vinculante urgente, según el caso, del Comité, cuando una autoridad de control competente no haya tomado una medida apropiada en una situación en la que sea urgente intervenir a fin de proteger los derechos y las libertades de los interesados.

4. No obstante lo dispuesto en el artículo 64, apartado 3, y en el artículo 65, apartado 2, los dictámenes urgentes o decisiones vinculantes urgentes contemplados en los apartados 2 y 3 del presente artículo se adoptarán en el plazo de dos semanas por mayoría simple de los miembros del Comité.

Artículo 67. *Intercambio de información.*

La Comisión podrá adoptar actos de ejecución de ámbito general para especificar las modalidades de intercambio de información por medios electrónicos entre las autoridades de control, y entre dichas autoridades y el Comité, en especial el formato normalizado contemplado en el artículo 64.

Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.

Sección 3. Comité europeo de protección de datos

Artículo 68. *Comité Europeo de Protección de Datos.*

1. Se crea el Comité Europeo de Protección de Datos («Comité»), como organismo de la Unión, que gozará de personalidad jurídica.

2. El Comité estará representado por su presidente.

3. El Comité estará compuesto por el director de una autoridad de control de cada Estado miembro y por el Supervisor Europeo de Protección de Datos o sus representantes respectivos.

4. Cuando en un Estado miembro estén encargados de controlar la aplicación de las disposiciones del presente Reglamento varias autoridades de control, se nombrará a un representante común de conformidad con el Derecho de ese Estado miembro.

5. La Comisión tendrá derecho a participar en las actividades y reuniones del Comité, sin derecho a voto. La Comisión designará un representante. El presidente del Comité comunicará a la Comisión las actividades del Comité.

6. En los casos a que se refiere el artículo 65, el Supervisor Europeo de Protección de Datos sólo tendrá derecho a voto en las decisiones relativas a los principios y normas

aplicables a las instituciones, órganos y organismos de la Unión que correspondan en cuanto al fondo a las contempladas en el presente Reglamento.

Artículo 69. *Independencia.*

1. El Comité actuará con total independencia en el desempeño de sus funciones o el ejercicio de sus competencias con arreglo a los artículos 70 y 71.

2. Sin perjuicio de las solicitudes de la Comisión contempladas en el artículo 70, apartados 1 y 2, el Comité no solicitará ni admitirá instrucciones de nadie en el desempeño de sus funciones o el ejercicio de sus competencias.

Artículo 70. *Funciones del Comité.*

1. El Comité garantizará la aplicación coherente del presente Reglamento. A tal efecto, el Comité, a iniciativa propia o, en su caso, a instancia de la Comisión, en particular:

a) supervisará y garantizará la correcta aplicación del presente Reglamento en los casos contemplados en los artículos 64 y 65, sin perjuicio de las funciones de las autoridades de control nacionales;

b) asesorará a la Comisión sobre toda cuestión relativa a la protección de datos personales en la Unión, en particular sobre cualquier propuesta de modificación del presente Reglamento;

c) asesorará a la Comisión sobre el formato y los procedimientos para intercambiar información entre los responsables, los encargados y las autoridades de control en relación con las normas corporativas vinculantes;

d) emitirá directrices, recomendaciones y buenas prácticas relativas a los procedimientos para la supresión de vínculos, copias o réplicas de los datos personales procedentes de servicios de comunicación a disposición pública a que se refiere el artículo 17, apartado 2;

e) examinará, a iniciativa propia, a instancia de uno de sus miembros o de la Comisión, cualquier cuestión relativa a la aplicación del presente Reglamento, y emitirá directrices, recomendaciones y buenas prácticas a fin de promover la aplicación coherente del presente Reglamento;

f) emitirá directrices, recomendaciones y buenas prácticas de conformidad con la letra e) del presente apartado a fin de especificar más los criterios y requisitos de las decisiones basadas en perfiles en virtud del artículo 22, apartado 2;

g) emitirá directrices, recomendaciones y buenas prácticas con arreglo a la letra e) del presente apartado a fin de constatar las violaciones de la seguridad de los datos y determinar la dilación indebida a tenor del artículo 33, apartados 1 y 2, y con respecto a las circunstancias particulares en las que el responsable o el encargado del tratamiento debe notificar la violación de la seguridad de los datos personales;

h) emitirá directrices, recomendaciones y buenas prácticas con arreglo a la letra e) del presente apartado con respecto a las circunstancias en las que sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas a tenor del artículo 34, apartado 1;

i) emitirá directrices, recomendaciones y buenas prácticas con arreglo a la letra e) del presente apartado con el fin de especificar en mayor medida los criterios y requisitos para las transferencias de datos personales basadas en normas corporativas vinculantes a las que se hayan adherido los responsables del tratamiento y en normas corporativas vinculantes a las que se hayan adherido los encargados del tratamiento y en requisitos adicionales necesarios para garantizar la protección de los datos personales de los interesados a que se refiere el artículo 47;

j) emitirá directrices, recomendaciones y buenas prácticas con arreglo a la letra e) del presente apartado a fin de especificar en mayor medida los criterios y requisitos de las transferencias de datos personales sobre la base del artículo 49, apartado 1;

k) formulará directrices para las autoridades de control, relativas a la aplicación de las medidas a que se refiere el artículo 58, apartados 1, 2 y 3, y la fijación de multas administrativas de conformidad con el artículo 83;

l) examinará la aplicación práctica de las directrices, recomendaciones y buenas prácticas;

m) emitirá directrices, recomendaciones y buenas prácticas con arreglo a la letra e) del presente apartado a fin de establecer procedimientos comunes de información procedente de personas físicas sobre infracciones del presente Reglamento en virtud del artículo 54, apartado 2;

n) alentará la elaboración de códigos de conducta y el establecimiento de mecanismos de certificación de la protección de datos y de sellos y marcas de protección de datos de conformidad con los artículos 40 y 42;

o) aprobará los criterios de certificación en virtud del artículo 42, apartado 5, y llevará un registro público de los mecanismos de certificación y sellos y marcas de protección de datos en virtud del artículo 42, apartado 8, y de los responsables o los encargados del tratamiento certificados establecidos en terceros países en virtud del artículo 42, apartado 7;

p) aprobará los requisitos contemplados en el artículo 43, apartado 3, con miras a la acreditación de los organismos de certificación a los que se refiere el artículo 43;

q) facilitará a la Comisión un dictamen sobre los requisitos de certificación contemplados en el artículo 43, apartado 8;

r) facilitará a la Comisión un dictamen sobre los iconos a que se refiere el artículo 12, apartado 7;

s) facilitará a la Comisión un dictamen para evaluar la adecuación del nivel de protección en un tercer país u organización internacional, en particular para evaluar si un tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o una organización internacional, ya no garantizan un nivel de protección adecuado. A tal fin, la Comisión facilitará al Comité toda la documentación necesaria, incluida la correspondencia con el gobierno del tercer país, que se refiera a dicho tercer país, territorio o específico o a dicha organización internacional;

t) emitirá dictámenes sobre los proyectos de decisión de las autoridades de control en virtud del mecanismo de coherencia mencionado en el artículo 64, apartado 1, sobre los asuntos presentados en virtud del artículo 64, apartado 2, y sobre las decisiones vinculantes en virtud del artículo 65, incluidos los casos mencionados en el artículo 66;

u) promoverá la cooperación y los intercambios bilaterales y multilaterales efectivos de información y de buenas prácticas entre las autoridades de control;

v) promoverá programas de formación comunes y facilitará intercambios de personal entre las autoridades de control y, cuando proceda, con las autoridades de control de terceros países o con organizaciones internacionales;

w) promoverá el intercambio de conocimientos y documentación sobre legislación y prácticas en materia de protección de datos con las autoridades de control encargadas de la protección de datos a escala mundial;

x) emitirá dictámenes sobre los códigos de conducta elaborados a escala de la Unión de conformidad con el artículo 40, apartado 9, y

y) llevará un registro electrónico, de acceso público, de las decisiones adoptadas por las autoridades de control y los tribunales sobre los asuntos tratados en el marco del mecanismo de coherencia.

2. Cuando la Comisión solicite asesoramiento del Comité podrá señalar un plazo teniendo en cuenta la urgencia del asunto.

3. El Comité transmitirá sus dictámenes, directrices, recomendaciones y buenas prácticas a la Comisión y al Comité contemplado en el artículo 93, y los hará públicos.

4. Cuando proceda, el Comité consultará a las partes interesadas y les dará la oportunidad de presentar sus comentarios en un plazo razonable. Sin perjuicio de lo dispuesto en el artículo 76, el Comité publicará los resultados del procedimiento de consulta.

Artículo 71. *Informes.*

1. El Comité elaborará un informe anual en materia de protección de las personas físicas en lo que respecta al tratamiento en la Unión y, si procede, en terceros países y organizaciones internacionales. El informe se hará público y se transmitirá al Parlamento Europeo, al Consejo y a la Comisión.

2. El informe anual incluirá un examen de la aplicación práctica de las directrices, recomendaciones y buenas prácticas indicadas en el artículo 70, apartado 1, letra l), así como de las decisiones vinculantes indicadas en el artículo 65.

Artículo 72. *Procedimiento.*

1. El Comité tomará sus decisiones por mayoría simple de sus miembros, salvo que el presente Reglamento disponga otra cosa.
2. El Comité adoptará su reglamento interno por mayoría de dos tercios de sus miembros y organizará sus disposiciones de funcionamiento.

Artículo 73. *Presidencia.*

1. El Comité elegirá por mayoría simple de entre sus miembros un presidente y dos vicepresidentes.
2. El mandato del presidente y de los vicepresidentes será de cinco años de duración y podrá renovarse una vez.

Artículo 74. *Funciones del presidente.*

1. El presidente desempeñará las siguientes funciones:

a) convocar las reuniones del Comité y preparar su orden del día;
b) notificar las decisiones adoptadas por el Comité con arreglo al artículo 65 a la autoridad de control principal y a las autoridades de control interesadas;
c) garantizar el ejercicio puntual de las funciones del Comité, en particular en relación con el mecanismo de coherencia a que se refiere el artículo 63.

2. El Comité determinará la distribución de funciones entre el presidente y los vicepresidentes en su reglamento interno.

Artículo 75. *Secretaría.*

1. El Comité contará con una secretaría, de la que se hará cargo el Supervisor Europeo de Protección de Datos.
2. La secretaría ejercerá sus funciones siguiendo exclusivamente las instrucciones del presidente del Comité.
3. El personal del Supervisor Europeo de Protección de Datos que participe en el desempeño de las funciones conferidas al Comité por el presente Reglamento dependerá de un superior jerárquico distinto del personal que desempeñe las funciones conferidas al Supervisor Europeo de Protección de Datos.
4. El Comité, en consulta con el Supervisor Europeo de Protección de Datos, elaborará y publicará, si procede, un memorando de entendimiento para la puesta en práctica del presente artículo, que determinará los términos de su cooperación y que será aplicable al personal del Supervisor Europeo de Protección de Datos que participe en el desempeño de las funciones conferidas al Comité por el presente Reglamento.
5. La secretaría prestará apoyo analítico, administrativo y logístico al Comité.
6. La secretaría será responsable, en particular, de:

a) los asuntos corrientes del Comité;
b) la comunicación entre los miembros del Comité, su presidente y la Comisión;
c) la comunicación con otras instituciones y con el público;
d) la utilización de medios electrónicos para la comunicación interna y externa;
e) la traducción de la información pertinente;
f) la preparación y el seguimiento de las reuniones del Comité;
g) la preparación, redacción y publicación de dictámenes, decisiones relativas a solución de diferencias entre autoridades de control y otros textos adoptados por el Comité.

Artículo 76. *Confidencialidad.*

1. Los debates del Comité serán confidenciales cuando el mismo lo considere necesario, tal como establezca su reglamento interno.

2. El acceso a los documentos presentados a los miembros del Comité, los expertos y los representantes de terceras partes se regirá por el Reglamento (CE) n.º 1049/2001 del Parlamento Europeo y del Consejo [21].

[21] Reglamento (CE) n.º 1049/2001 del Parlamento Europeo y del Consejo, de 30 de mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión (DO L 145 de 31.5.2001, p. 43).

CAPÍTULO VIII

Recursos, responsabilidad y sanciones

Artículo 77. *Derecho a presentar una reclamación ante una autoridad de control.*

1. Sin perjuicio de cualquier otro recurso administrativo o acción judicial, todo interesado tendrá derecho a presentar una reclamación ante una autoridad de control, en particular en el Estado miembro en el que tenga su residencia habitual, lugar de trabajo o lugar de la supuesta infracción, si considera que el tratamiento de datos personales que le conciernen infringe el presente Reglamento.

2. La autoridad de control ante la que se haya presentado la reclamación informará al reclamante sobre el curso y el resultado de la reclamación, inclusive sobre la posibilidad de acceder a la tutela judicial en virtud del artículo 78.

Artículo 78. *Derecho a la tutela judicial efectiva contra una autoridad de control.*

1. Sin perjuicio de cualquier otro recurso administrativo o extrajudicial, toda persona física o jurídica tendrá derecho a la tutela judicial efectiva contra una decisión jurídicamente vinculante de una autoridad de control que le concierna.

2. Sin perjuicio de cualquier otro recurso administrativo o extrajudicial, todo interesado tendrá derecho a la tutela judicial efectiva en caso de que la autoridad de control que sea competente en virtud de los artículos 55 y 56 no dé curso a una reclamación o no informe al interesado en el plazo de tres meses sobre el curso o el resultado de la reclamación presentada en virtud del artículo 77.

3. Las acciones contra una autoridad de control deberán ejercitarse ante los tribunales del Estado miembro en que esté establecida la autoridad de control.

4. Cuando se ejerciten acciones contra una decisión de una autoridad de control que haya sido precedida de un dictamen o una decisión del Comité en el marco del mecanismo de coherencia, la autoridad de control remitirá al tribunal dicho dictamen o decisión.

Artículo 79. *Derecho a la tutela judicial efectiva contra un responsable o encargado del tratamiento.*

1. Sin perjuicio de los recursos administrativos o extrajudiciales disponibles, incluido el derecho a presentar una reclamación ante una autoridad de control en virtud del artículo 77, todo interesado tendrá derecho a la tutela judicial efectiva cuando considere que sus derechos en virtud del presente Reglamento han sido vulnerados como consecuencia de un tratamiento de sus datos personales.

2. Las acciones contra un responsable o encargado del tratamiento deberán ejercitarse ante los tribunales del Estado miembro en el que el responsable o encargado tenga un establecimiento. Alternativamente, tales acciones podrán ejercitarse ante los tribunales del Estado miembro en que el interesado tenga su residencia habitual, a menos que el responsable o el encargado sea una autoridad pública de un Estado miembro que actúe en ejercicio de sus poderes públicos.

Artículo 80. *Representación de los interesados.*

1. El interesado tendrá derecho a dar mandato a una entidad, organización o asociación sin ánimo de lucro que haya sido correctamente constituida con arreglo al Derecho de un Estado miembro, cuyos objetivos estatutarios sean de interés público y que actúe en el

ámbito de la protección de los derechos y libertades de los interesados en materia de protección de sus datos personales, para que presente en su nombre la reclamación, y ejerza en su nombre los derechos contemplados en los artículos 77, 78 y 79, y el derecho a ser indemnizado mencionado en el artículo 82 si así lo establece el Derecho del Estado miembro.

2. Cualquier Estado miembro podrán disponer que cualquier entidad, organización o asociación mencionada en el apartado 1 del presente artículo tenga, con independencia del mandato del interesado, derecho a presentar en ese Estado miembro una reclamación ante la autoridad de control que sea competente en virtud del artículo 77 y a ejercer los derechos contemplados en los artículos 78 y 79, si considera que los derechos del interesado con arreglo al presente Reglamento han sido vulnerados como consecuencia de un tratamiento.

Artículo 81. *Suspensión de los procedimientos.*

1. Cuando un tribunal competente de un Estado miembro tenga información de la pendencia ante un tribunal de otro Estado miembro de un procedimiento relativo a un mismo asunto en relación con el tratamiento por el mismo responsable o encargado, se pondrá en contacto con dicho tribunal de otro Estado miembro para confirmar la existencia de dicho procedimiento.

2. Cuando un procedimiento relativo a un mismo asunto en relación con el tratamiento por el mismo responsable o encargado esté pendiente ante un tribunal de otro Estado miembro, cualquier tribunal competente distinto de aquel ante el que se ejercitó la acción en primer lugar podrá suspender su procedimiento.

3. Cuando dicho procedimiento esté pendiente en primera instancia, cualquier tribunal distinto de aquel ante el que se ejercitó la acción en primer lugar podrá también, a instancia de una de las partes, inhibirse en caso de que el primer tribunal sea competente para su conocimiento y su acumulación sea conforme a Derecho.

Artículo 82. *Derecho a indemnización y responsabilidad.*

1. Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente Reglamento tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos.

2. Cualquier responsable que participe en la operación de tratamiento responderá de los daños y perjuicios causados en caso de que dicha operación no cumpla lo dispuesto por el presente Reglamento. Un encargado únicamente responderá de los daños y perjuicios causados por el tratamiento cuando no haya cumplido con las obligaciones del presente Reglamento dirigidas específicamente a los encargados o haya actuado al margen o en contra de las instrucciones legales del responsable.

3. El responsable o encargado del tratamiento estará exento de responsabilidad en virtud del apartado 2 si demuestra que no es en modo alguno responsable del hecho que haya causado los daños y perjuicios.

4. Cuando más de un responsable o encargado del tratamiento, o un responsable y un encargado hayan participado en la misma operación de tratamiento y sean, con arreglo a los apartados 2 y 3, responsables de cualquier daño o perjuicio causado por dicho tratamiento, cada responsable o encargado será considerado responsable de todos los daños y perjuicios, a fin de garantizar la indemnización efectiva del interesado.

5. Cuando, de conformidad con el apartado 4, un responsable o encargado del tratamiento haya pagado una indemnización total por el perjuicio ocasionado, dicho responsable o encargado tendrá derecho a reclamar a los demás responsables o encargados que hayan participado en esa misma operación de tratamiento la parte de la indemnización correspondiente a su parte de responsabilidad por los daños y perjuicios causados, de conformidad con las condiciones fijadas en el apartado 2.

6. Las acciones judiciales en ejercicio del derecho a indemnización se presentarán ante los tribunales competentes con arreglo al Derecho del Estado miembro que se indica en el artículo 79, apartado 2.

Artículo 83. *Condiciones generales para la imposición de multas administrativas.*

1. Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 5 y 6 sean en cada caso individual efectivas, proporcionadas y disuasorias.

2. Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j). Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta:

a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;

b) la intencionalidad o negligencia en la infracción;

c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;

d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32;

e) toda infracción anterior cometida por el responsable o el encargado del tratamiento;

f) el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;

g) las categorías de los datos de carácter personal afectados por la infracción;

h) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida;

i) cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas;

j) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42, y

k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción.

3. Si un responsable o un encargado del tratamiento incumpliera de forma intencionada o negligente, para las mismas operaciones de tratamiento u operaciones vinculadas, diversas disposiciones del presente Reglamento, la cuantía total de la multa administrativa no será superior a la cuantía prevista para las infracciones más graves.

4. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43;

b) las obligaciones de los organismos de certificación a tenor de los artículos 42 y 43;

c) las obligaciones del organismo de supervisión a tenor del artículo 41, apartado 4.

5. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9;

b) los derechos de los interesados a tenor de los artículos 12 a 22;

c) las transferencias de datos personales a un destinatario en un tercer país o una organización internacional a tenor de los artículos 44 a 49;

d) toda obligación en virtud del Derecho de los Estados miembros que se adopte con arreglo al capítulo IX;

e) el incumplimiento de una resolución o de una limitación temporal o definitiva del tratamiento o la suspensión de los flujos de datos por parte de la autoridad de control con arreglo al artículo 58, apartado 2, o el no facilitar acceso en incumplimiento del artículo 58, apartado 1.

6. El incumplimiento de las resoluciones de la autoridad de control a tenor del artículo 58, apartado 2, se sancionará de acuerdo con el apartado 2 del presente artículo con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.

7. Sin perjuicio de los poderes correctivos de las autoridades de control en virtud del artículo 58, apartado 2, cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro.

8. El ejercicio por una autoridad de control de sus poderes en virtud del presente artículo estará sujeto a garantías procesales adecuadas de conformidad con el Derecho de la Unión y de los Estados miembros, entre ellas la tutela judicial efectiva y el respeto de las garantías procesales.

9. Cuando el ordenamiento jurídico de un Estado miembro no establezca multas administrativas, el presente artículo podrá aplicarse de tal modo que la incoación de la multa corresponda a la autoridad de control competente y su imposición a los tribunales nacionales competentes, garantizando al mismo tiempo que estas vías de derecho sean efectivas y tengan un efecto equivalente a las multas administrativas impuestas por las autoridades de control. En cualquier caso, las multas impuestas serán efectivas, proporcionadas y disuasorias. Los Estados miembros de que se trate notificarán a la Comisión las disposiciones legislativas que adopten en virtud del presente apartado a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier ley de modificación o modificación posterior que les sea aplicable.

Artículo 84. *Sanciones.*

1. Los Estados miembros establecerán las normas en materia de otras sanciones aplicables a las infracciones del presente Reglamento, en particular las infracciones que no se sancionen con multas administrativas de conformidad con el artículo 83, y adoptarán todas las medidas necesarias para garantizar su observancia. Dichas sanciones serán efectivas, proporcionadas y disuasorias.

2. Cada Estado miembro notificará a la Comisión las disposiciones legislativas que adopte de conformidad con el apartado 1 a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier modificación posterior que les sea aplicable.

CAPÍTULO IX

Disposiciones relativas a situaciones específicas de tratamiento

Artículo 85. *Tratamiento y libertad de expresión y de información.*

1. Los Estados miembros conciliarán por ley el derecho a la protección de los datos personales en virtud del presente Reglamento con el derecho a la libertad de expresión y de información, incluido el tratamiento con fines periodísticos y fines de expresión académica, artística o literaria.

2. Para el tratamiento realizado con fines periodísticos o con fines de expresión académica, artística o literaria, los Estados miembros establecerán exenciones o excepciones de lo dispuesto en los capítulos II (principios), III (derechos del interesado), IV (responsable y encargado del tratamiento), V (transferencia de datos personales a terceros países u organizaciones internacionales), VI (autoridades de control independientes), VII (cooperación y coherencia) y IX (disposiciones relativas a situaciones específicas de tratamiento de datos), si son necesarias para conciliar el derecho a la protección de los datos personales con la libertad de expresión e información.

3. Cada Estado miembro notificará a la Comisión las disposiciones legislativas que adopte de conformidad con el apartado 2 y, sin dilación, cualquier modificación posterior, legislativa u otra, de las mismas.

Artículo 86. *Tratamiento y acceso del público a documentos oficiales.*

Los datos personales de documentos oficiales en posesión de alguna autoridad pública o u organismo público o una entidad privada para la realización de una misión en interés público podrán ser comunicados por dicha autoridad, organismo o entidad de conformidad con el Derecho de la Unión o de los Estados miembros que se les aplique a fin de conciliar el acceso del público a documentos oficiales con el derecho a la protección de los datos personales en virtud del presente Reglamento.

Artículo 87. *Tratamiento del número nacional de identificación.*

Los Estados miembros podrán determinar adicionalmente las condiciones específicas para el tratamiento de un número nacional de identificación o cualquier otro medio de identificación de carácter general. En ese caso, el número nacional de identificación o cualquier otro medio de identificación de carácter general se utilizará únicamente con las garantías adecuadas para los derechos y las libertades del interesado con arreglo al presente Reglamento.

Artículo 88. *Tratamiento en el ámbito laboral.*

1. Los Estados miembros podrán, a través de disposiciones legislativas o de convenios colectivos, establecer normas más específicas para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral, en particular a efectos de contratación de personal, ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por el convenio colectivo, gestión, planificación y organización del trabajo, igualdad y diversidad en el lugar de trabajo, salud y seguridad en el trabajo, protección de los bienes de empleadores o clientes, así como a efectos del ejercicio y disfrute, individual o colectivo, de los derechos y prestaciones relacionados con el empleo y a efectos de la extinción de la relación laboral.

2. Dichas normas incluirán medidas adecuadas y específicas para preservar la dignidad humana de los interesados así como sus intereses legítimos y sus derechos fundamentales, prestando especial atención a la transparencia del tratamiento, a la transferencia de los datos personales dentro de un grupo empresarial o de una unión de empresas dedicadas a una actividad económica conjunta y a los sistemas de supervisión en el lugar de trabajo.

3. Cada Estado miembro notificará a la Comisión las disposiciones legales que adopte de conformidad con el apartado 1 a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier modificación posterior de las mismas.

Artículo 89. *Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.*

1. El tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos estará sujeto a las garantías adecuadas, con arreglo al presente Reglamento, para los derechos y las libertades de los interesados. Dichas garantías harán que se disponga de medidas técnicas y organizativas, en particular para garantizar el respeto del principio de minimización de los datos personales. Tales medidas podrán incluir la seudonimización, siempre que de esa forma puedan alcanzarse dichos fines. Siempre que esos fines pueden alcanzarse mediante un tratamiento ulterior que no permita o ya no permita la identificación de los interesados, esos fines se alcanzarán de ese modo.

2. Cuando se traten datos personales con fines de investigación científica o histórica o estadísticos el Derecho de la Unión o de los Estados miembros podrá establecer excepciones a los derechos contemplados en los artículos 15, 16, 18 y 21, sujetas a las condiciones y garantías indicadas en el apartado 1 del presente artículo, siempre y cuando sea probable que esos derechos imposibiliten u obstaculicen gravemente el logro de los fines científicos y cuando esas excepciones sean necesarias para alcanzar esos fines.

3. Cuando se traten datos personales con fines de archivo en interés público, el Derecho de le Unión o de los Estados miembros podrá prever excepciones a los derechos contemplados en los artículos 15, 16, 18, 19, 20 y 21, sujetas a las condiciones y garantías citadas en el apartado 1 del presente artículo, siempre que esos derechos puedan imposibilitar u obstaculizar gravemente el logro de los fines científicos y cuanto esas excepciones sean necesarias para alcanzar esos fines.

4. En caso de que el tratamiento a que hacen referencia los apartados 2 y 3 sirva también al mismo tiempo a otro fin, las excepciones solo serán aplicables al tratamiento para los fines mencionados en dichos apartados.

Artículo 90. *Obligaciones de secreto.*

1. Los Estados miembros podrán adoptar normas específicas para fijar los poderes de las autoridades de control establecidos en el artículo 58, apartado 1, letras e) y f), en relación con los responsables o encargados sujetos, con arreglo al Derecho de la Unión o de los Estados miembros o a las normas establecidas por los organismos nacionales competentes, a una obligación de secreto profesional o a otras obligaciones de secreto equivalentes, cuando sea necesario y proporcionado para conciliar el derecho a la protección de los datos personales con la obligación de secreto. Esas normas solo se aplicarán a los datos personales que el responsable o el encargado del tratamiento hayan recibido como resultado o con ocasión de una actividad cubierta por la citada obligación de secreto.

2. Cada Estado miembro notificará a la Comisión las normas adoptadas de conformidad con el apartado 1 a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier modificación posterior de las mismas.

Artículo 91. *Normas vigentes sobre protección de datos de las iglesias y asociaciones religiosas.*

1. Cuando en un Estado miembro iglesias, asociaciones o comunidades religiosas apliquen, en el momento de la entrada en vigor del presente Reglamento, un conjunto de normas relativas a la protección de las personas físicas en lo que respecta al tratamiento, tales normas podrán seguir aplicándose, siempre que sean conformes con el presente Reglamento.

2. Las iglesias y las asociaciones religiosas que apliquen normas generales de conformidad con el apartado 1 del presente artículo estarán sujetas al control de una autoridad de control independiente, que podrá ser específica, siempre que cumpla las condiciones establecidas en el capítulo VI del presente Reglamento.

CAPÍTULO X

Actos delegados y actos de ejecución

Artículo 92. *Ejercicio de la delegación.*

1. Los poderes para adoptar actos delegados otorgados a la Comisión estarán sujetos a las condiciones establecidas en el presente artículo.

2. La delegación de poderes indicada en el artículo 12, apartado 8, y en el artículo 43, apartado 8, se otorgarán a la Comisión por tiempo indefinido a partir del 24 de mayo de 2016.

3. La delegación de poderes mencionada en el artículo 12, apartado 8, y el artículo 43, apartado 8, podrá ser revocada en cualquier momento por el Parlamento Europeo o por el Consejo. La decisión de revocación pondrá término a la delegación de los poderes que en ella se especifiquen. La decisión surtirá efecto al día siguiente de su publicación en el Diario Oficial de la Unión Europea o en una fecha posterior indicada en la misma. No afectará a la validez de los actos delegados que ya estén en vigor.

4. Tan pronto como la Comisión adopte un acto delegado lo notificará simultáneamente al Parlamento Europeo y al Consejo.

5. Los actos delegados adoptados en virtud del artículo 12, apartado 8, y el artículo 43, apartado 8, entrarán en vigor únicamente si, en un plazo de tres meses desde su notificación

al Parlamento Europeo y al Consejo, ni el Parlamento Europeo ni el Consejo formulan objeciones o si, antes del vencimiento de dicho plazo, tanto el uno como el otro informan a la Comisión de que no las formularán. El plazo se ampliará en tres meses a iniciativa del Parlamento Europeo o del Consejo.

Artículo 93. *Procedimiento de comité.*

1. La Comisión estará asistida por un comité. Dicho comité será un comité en el sentido del Reglamento (UE) n.º 182/2011.
2. Cuando se haga referencia al presente apartado, se aplicará el artículo 5 del Reglamento (UE) n.º 182/2011.
3. Cuando se haga referencia al presente apartado, se aplicará el artículo 8 del Reglamento (UE) n.º 182/2011, en relación con su artículo 5.

CAPÍTULO XI

Disposiciones finales

Artículo 94. *Derogación de la Directiva 95/46/CE.*

1. Queda derogada la Directiva 95/46/CE con efecto a partir del 25 de mayo de 2018.
2. Toda referencia a la Directiva derogada se entenderá hecha al presente Reglamento. Toda referencia al Grupo de protección de las personas en lo que respecta al tratamiento de datos personales establecido por el artículo 29 de la Directiva 95/46/CE se entenderá hecha al Comité Europeo de Protección de Datos establecido por el presente Reglamento.

Artículo 95. *Relación con la Directiva 2002/58/CE.*

El presente Reglamento no impondrá obligaciones adicionales a las personas físicas o jurídicas en materia de tratamiento en el marco de la prestación de servicios públicos de comunicaciones electrónicas en redes públicas de comunicación de la Unión en ámbitos en los que estén sujetas a obligaciones específicas con el mismo objetivo establecidas en la Directiva 2002/58/CE.

Artículo 96. *Relación con acuerdos celebrados anteriormente.*

Los acuerdos internacionales que impliquen la transferencia de datos personales a terceros países u organizaciones internacionales que hubieren sido celebrados por los Estados miembros antes del 24 de mayo de 2016 y que cumplan lo dispuesto en el Derecho de la Unión aplicable antes de dicha fecha, seguirán en vigor hasta que sean modificados, sustituidos o revocados.

Artículo 97. *Informes de la Comisión.*

1. A más tardar el 25 de mayo de 2020 y posteriormente cada cuatro años, la Comisión presentará al Parlamento Europeo y al Consejo un informe sobre la evaluación y revisión del presente Reglamento. Los informes se harán públicos.
2. En el marco de las evaluaciones y revisiones a que se refiere el apartado 1, la Comisión examinará en particular la aplicación y el funcionamiento de:

a) el capítulo V sobre la transferencia de datos personales a países terceros u organizaciones internacionales, particularmente respecto de las decisiones adoptadas en virtud del artículo 45, apartado 3, del presente Reglamento, y de las adoptadas sobre la base del artículo 25, apartado 6, de la Directiva 95/46/CE;
b) el capítulo VII sobre cooperación y coherencia.

3. A los efectos del apartado 1, la Comisión podrá solicitar información a los Estados miembros y a las autoridades de control.
4. Al llevar a cabo las evaluaciones y revisiones indicadas en los apartados 1 y 2, la Comisión tendrá en cuenta las posiciones y conclusiones del Parlamento Europeo, el Consejo y los demás órganos o fuentes pertinentes.

5. La Comisión presentará, en caso necesario, las propuestas oportunas para modificar el presente Reglamento, en particular teniendo en cuenta la evolución de las tecnologías de la información y a la vista de los progresos en la sociedad de la información.

Artículo 98. *Revisión de otros actos jurídicos de la Unión en materia de protección de datos.*

La Comisión presentará, si procede, propuestas legislativas para modificar otros actos jurídicos de la Unión en materia de protección de datos personales, a fin de garantizar la protección uniforme y coherente de las personas físicas en relación con el tratamiento. Se tratará en particular de las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento por parte de las instituciones, órganos, y organismos de la Unión y a la libre circulación de tales datos.

Artículo 99. *Entrada en vigor y aplicación.*

1. El presente Reglamento entrará en vigor a los veinte días de su publicación en el Diario Oficial de la Unión Europea.
2. Será aplicable a partir del 25 de mayo de 2018.

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

§ 54

Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 126, de 27 de mayo de 2021
Última modificación: 29 de julio de 2022
Referencia: BOE-A-2021-8806

FELIPE VI

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley orgánica:

PREÁMBULO

I

La Unión Europea es un espacio en el que los estándares y las garantías de protección de los derechos de las personas físicas a la protección de los datos personales se encuentran en la vanguardia internacional y constituyen un referente mundial. El rápido desarrollo tecnológico, especialmente de Internet, así como la creciente globalización de la economía mundial y europea han hecho imprescindible abordar la reforma del marco jurídico de la protección de datos, al objeto de consolidar e incluso mejorar este elevado nivel de protección a través de la creación de un marco legislativo nuevo, adaptado a la realidad cambiante, al tiempo que sólido, coherente e integral. En definitiva, un entorno normativo para un mundo globalizado y digital.

En este sentido, la Comunicación de la Comisión Europea «Un enfoque global de la protección de los datos personales en la Unión Europea», de 4 de noviembre de 2010, precedida de un intenso periodo de consultas durante más de dos años con los Estados miembros, el público en general, así como con los distintos sectores afectados, sentó las bases de lo que sería esta nueva perspectiva normativa.

El marco normativo resultante consta, principalmente, de dos instrumentos: el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos), que sustituye a una norma vigente

desde hacía más de veinte años, y la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

En nuestro ordenamiento jurídico, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, adaptó el Reglamento General de Protección de Datos, en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos.

II

La Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, objeto de transposición por esta Ley Orgánica, deroga la Decisión Marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal, que había sido superada por varias razones.

En primer lugar, se trataba de una norma previa al Tratado de Lisboa que requería de su oportuna adaptación a los nuevos Tratados, en particular, al artículo 16 del Tratado de Funcionamiento de la Unión Europea, que exige que el Consejo y el Parlamento Europeo, a través del procedimiento legislativo ordinario, regulen la protección de los datos personales.

En segundo término, la decisión marco se aprobó conforme a la estructura de pilares de la Unión Europea, previa al Tratado de Lisboa, por lo que contaba con un ámbito de aplicación limitado exclusivamente al tratamiento de datos personales de carácter transfronterizo entre los Estados miembros, sin alcanzar, por tanto, a los tratamientos de carácter estrictamente nacional.

Asimismo, otorgaba una amplísima capacidad de maniobra a los Estados miembros, sin asegurar un nivel mínimo de armonización deseable en determinados ámbitos, como el reconocimiento en todos los Estados del derecho de acceso de los interesados a sus propios datos, el principio del tratamiento de los datos para fines determinados o las condiciones para las transferencias internacionales.

En definitiva, la fragmentación y complejidad de la regulación en este campo perjudicaba la necesaria confianza entre los actores de la cooperación policial y judicial penal en Europa, quienes mostraban recelos a compartir información, entre otros motivos, por la ausencia de una mínima armonización en cuanto a la protección de los datos de carácter personal; unos datos que resultan esenciales en el terreno de la cooperación operativa.

III

La Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, subsana estas deficiencias, ampliando su ámbito de aplicación al tratamiento nacional de los datos personales en el espacio de la cooperación policial y judicial penal. Toda vez que cubre otras carencias de la normativa europea anterior, dado que incluye la regulación de los datos genéticos –que reclamaba el Tribunal Europeo de Derechos Humanos-, así como la distinción entre los datos personales según su grado de exactitud y fiabilidad, o la diferenciación entre distintas categorías de interesados.

Resulta pertinente poner de relieve que la citada directiva que transpone esta Ley Orgánica se aprobó como respuesta a las crecientes amenazas para la seguridad en el contexto nacional e internacional, que tienen, en numerosos casos, un componente transfronterizo. Por esta razón, la cooperación internacional y la transmisión de información de carácter personal entre los servicios policiales y judiciales de los países implicados se convierten en un objetivo ineludible. En efecto, los atentados terroristas de Nueva York en 2001 supusieron un punto de inflexión en la necesidad de reforzar la cooperación judicial y policial en la lucha contra el terrorismo, como volvería a ponerse de manifiesto con ocasión de los atentados de Bruselas y Niza en 2016.

La cooperación encaminada a compartir a tiempo la información operativa precisa se erige en un requisito de eficacia en la prevención y lucha contra este tipo de amenazas. Todo

ello, teniendo en cuenta el estado de la técnica, que permite, en la actualidad, tratamientos de datos a gran escala en el ámbito de la seguridad.

Este intercambio de información debe realizarse, en todo caso, de manera que se garanticen los principios democráticos y la seguridad de las personas a lo largo de las fases del tratamiento.

En consecuencia, esta Ley Orgánica asume la finalidad de lograr un elevado nivel de protección de los derechos de la ciudadanía, en general, y de sus datos personales, en particular, que resulte homologable al del resto de los Estados miembros de la Unión Europea, incorporando y concretando las reglas que establece la directiva.

En este sentido, la Constitución española fue precursora del reconocimiento y la defensa del derecho fundamental a la protección de datos personales. Así, el artículo 18.4 de nuestra norma fundamental dispone que la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de la ciudadanía y el pleno ejercicio de sus derechos. El Tribunal Constitucional, en reiterada jurisprudencia, entiende la protección de datos como un derecho fundamental que garantiza a toda persona la capacidad de controlar el uso y destino de sus datos, con el propósito de evitar el tráfico ilícito o lesivo de los mismos o una utilización para fines distintos de los que justificaron su obtención.

Por todo ello, la transposición de esta directiva por los Estados miembros supone el establecimiento de un marco jurídico consistente, que proporciona la seguridad jurídica necesaria para facilitar la cooperación policial y judicial penal y, por tanto, una mayor eficacia en el desempeño de sus funciones por las Fuerzas y Cuerpos de Seguridad y de nuestro sistema judicial penal en su conjunto, incluido el penitenciario.

IV

Esta Ley Orgánica consta de sesenta y cinco artículos estructurados en ocho capítulos, cinco disposiciones adicionales, una disposición transitoria, una disposición derogatoria y doce disposiciones finales.

El capítulo I, relativo a las disposiciones generales, define el objeto de la Ley Orgánica, entendiéndose como la regulación del tratamiento de los datos personales para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, incluida la protección y de prevención frente a las amenazas contra la seguridad pública, cuando dicho tratamiento se lleve a cabo por los órganos que, a efectos de esta Ley Orgánica, tengan la consideración de autoridades competentes.

La finalidad principal es que los datos sean tratados por estas autoridades competentes de manera que se cumplan los fines prevenidos a la par que establecer los mayores estándares de protección de los derechos fundamentales y las libertades de los ciudadanos, de forma que se cumpla lo dispuesto en el artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea, así como en el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea y el artículo 18.4 de la Constitución.

Asimismo, en correspondencia con lo que dispone el artículo 22.6 de la Ley Orgánica 3/2018, de 5 de diciembre, cuando el tratamiento de los datos personales se realice para alguno de los fines establecidos en esta Ley Orgánica y proceda de las imágenes y sonidos obtenidos mediante la utilización de cámaras y videocámaras por las Fuerzas y Cuerpos de Seguridad, o bien se lleve a cabo por los órganos competentes para la vigilancia y control en los centros penitenciarios o para el control, regulación, vigilancia y disciplina del tráfico, dichos tratamientos se regularán por las disposiciones de esta Ley Orgánica complementándose, en lo que no resulte contrario a su contenido, con la normativa vigente que regula estos ámbitos. De este modo, se establece un nuevo sistema que gira en torno a las obligaciones de los responsables del tratamiento y a las distintas misiones que se les asignan.

Aunque se deben excluir con carácter general, se incluyen igualmente algunas previsiones específicas para el tratamiento de los datos de personas fallecidas a similitud de lo que se dispone en la precitada Ley Orgánica 3/2018, de 5 de diciembre.

Las autoridades competentes, a efectos de esta Ley Orgánica, se definen como autoridades públicas con competencias legalmente encomendadas para la consecución de los fines específicos incluidos en el ámbito de aplicación. En concreto, se determina que serán autoridades competentes: las Fuerzas y Cuerpos de Seguridad; las autoridades

judiciales del orden jurisdiccional penal y el Ministerio Fiscal; las Administraciones Penitenciarias; la Dirección Adjunta de Vigilancia Aduanera; el Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias; y la Comisión de Vigilancia de Actividades de Financiación del Terrorismo. Todo ello, sin perjuicio de que los tratamientos que se lleven a cabo por los órganos jurisdiccionales se rijan por lo dispuesto en esta Ley Orgánica, en la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, y en las leyes procesales penales.

Se excluyen expresamente del ámbito de aplicación ciertos tratamientos, como los realizados por las autoridades competentes para fines distintos de los cubiertos por la Ley Orgánica; los llevados a cabo por los órganos de la Administración General del Estado en el marco de las actividades comprendidas en el ámbito del capítulo II del título V del Tratado de la Unión Europea, en relación a la Política Exterior y de Seguridad Común; los derivados de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión Europea; y los sometidos a la normativa sobre materias clasificadas. Entre estos últimos se mencionan expresamente como incluidos los tratamientos relativos a la Defensa Nacional.

El capítulo II se refiere a los principios de protección de datos cuya garantía corresponde al responsable del tratamiento. Estos principios se regulan en términos similares a lo establecido en el Reglamento General de Protección de Datos, con algunas especialidades propias del ámbito de esta Ley Orgánica.

Se incluye un deber de colaboración con las autoridades competentes, según el cual, salvo que legalmente sea exigible una autorización judicial, las Administraciones Públicas o cualquier persona física o jurídica deberá proporcionar a las autoridades judiciales, al Ministerio Fiscal o a la Policía Judicial la información necesaria para la investigación o enjuiciamiento de infracciones penales o la ejecución de las penas y la información necesaria para la protección y prevención frente a un peligro real y grave para la seguridad pública. Todo ello, con la obligación de no informar al interesado de dichos tratamientos ulteriores. Esta última precisión resulta fundamental para evitar que la puesta de la información a disposición del interesado pueda poner en peligro los fines que, de acuerdo con la directiva y esta Ley Orgánica, justifican el tratamiento de los datos.

Se regulan, también, los plazos de conservación y de revisión de los datos de carácter personal tratados, siendo relevante el establecimiento de un plazo máximo de conservación de los datos con carácter general y la implantación de un sistema que permite al responsable revisar, en el plazo que el mismo establezca dentro del margen legal, la necesidad de conservar, limitar o suprimir el conjunto de los datos personales contenidos en cada una de sus actividades de tratamiento. El responsable deberá, en sus tratamientos, distinguir los datos que correspondan a las diversas categorías de interesados, tales como los sospechosos, los condenados o los sancionados, las víctimas o los terceros involucrados, así como diferenciar, en la medida de lo posible, si los datos que trata son datos basados en hechos o en apreciaciones.

Se exigen igualmente ciertas condiciones que determinan la licitud de todo tratamiento de datos de carácter personal, esto es, que sean tratados por las autoridades competentes; que resulten necesarios para los fines de esta Ley Orgánica y que, en caso necesario y en cada ámbito particular, se especifiquen las especialidades por una norma con rango de ley que incluya unos contenidos mínimos.

En el supuesto de transmisión de datos sujetos a condiciones específicas de tratamiento, dichas condiciones deberán ser respetadas por el destinatario de los mismos, en especial, la prohibición de transmitirlos o de utilizarlos para fines distintos para los que fueron transmitidos.

De igual modo, se exige que el tratamiento de categorías especiales de datos, como son los que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical o los genéticos o biométricos, sólo pueda tener lugar cuando sea estrictamente necesario y se cumplan ciertas condiciones.

Los datos biométricos (como las huellas dactilares o la imagen facial) sólo se consideran incluidos en esta categoría especial cuando su tratamiento está dirigido a identificar de manera unívoca a una persona física. Esta necesidad de identificación en las actuaciones amparadas legalmente se lleva a cabo, con frecuencia, por las distintas autoridades competentes. El propósito es singularizar los autores o partícipes de infracciones penales,

así como poder reconocer si son las personas que se supone o se busca, y de esta forma, atribuir o exonerar, sin género de dudas, la participación en determinados hechos, gracias a posibles indicios o vestigios biométricos.

Habida cuenta de la vertiginosa evolución tecnológica y los medios electrónicos de los que se dispone, se incluye la habilitación legal que facilite una respuesta rápida y adecuada en el uso de estos datos, con el objetivo final de garantizar y proteger los derechos de los interesados y de la ciudadanía en general.

Se prohíbe, igualmente, la adopción de decisiones individuales automatizadas, incluida la elaboración de perfiles en este ámbito, salvo que esté autorizado por una norma con rango de ley del ordenamiento jurídico español o europeo.

El capítulo III, se divide en dos secciones y aborda los derechos de las personas. Regula una serie de condiciones generales del ejercicio de los derechos, tales como la obligación exigible al responsable de facilitar la información correspondiente a los derechos del interesado de forma concisa, con un lenguaje claro y sencillo y de manera gratuita. Se establece la información que debe ponerse a disposición del interesado, siendo algunos datos obligatorios, en todo caso, y otros en casos concretos.

Se reconocen los derechos de acceso, rectificación, supresión y limitación del tratamiento. En virtud de tales derechos se faculta al interesado a conocer si se están tratando o no sus datos y, en caso afirmativo, acceder a cierta información sobre el tratamiento; a obtener la rectificación de sus datos si estos resultaran inexactos; a suprimirlos cuando fueran contrarios a lo dispuesto en los artículos 6, 11 o 13, o cuando así lo requiera una obligación legal exigible al responsable; y a limitar el tratamiento, cuando el interesado ponga en duda la exactitud de los datos o estos datos deban conservarse únicamente a efectos probatorios.

Estos derechos podrán ser ejercidos por el interesado directamente o, en determinados casos, a través de la autoridad de protección de datos.

Dispone esta Ley Orgánica que estos derechos pueden ser restringidos por ciertas causas tasadas, como cuando sea necesario para evitar que se obstaculice una investigación o se ponga en peligro la seguridad pública o la seguridad nacional.

Se establece, en su sección segunda, un régimen especial de derechos de los interesados en el marco de investigaciones y procesos penales.

El capítulo IV recoge las obligaciones y responsabilidades de los responsables y encargados de protección de datos, las medidas de seguridad y la figura del delegado de protección de datos, a lo largo de tres secciones. El responsable del tratamiento, teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los niveles de riesgo para los derechos y libertades de las personas físicas, aplicará las medidas técnicas y organizativas apropiadas.

El encargado del tratamiento llevará a cabo sus funciones por cuenta del responsable, debiendo ofrecer garantías para aplicar medidas técnicas y organizativas apropiadas.

Todo responsable y encargado del tratamiento deberá conservar un registro de actividades de tratamiento, con datos identificativos, tales como los datos de contacto del responsable, los fines o las categorías de interesados, y un registro de operaciones, pieza angular de este sistema e instrumento básico para acreditar el cumplimiento de varios de los principios de tratamiento, que comprenderá la recogida, la alteración, las consultas y las transferencias de los datos personales entre otras operaciones. Asimismo, están obligados a cooperar con la autoridad de protección de datos, en el marco de la legislación vigente.

Se establecen ciertas obligaciones que responden a un nuevo modelo de responsabilidad activa que exige una valoración previa del riesgo que pudiera generar el tratamiento de los datos de carácter personal para los interesados, para, a partir de dicha valoración, adoptar las medidas que procedan.

Se presta una atención detallada a la seguridad del tratamiento, regulándose alguna de las medidas de seguridad que se aplicarán, si bien solo se dispone como obligatoria la puesta en marcha del citado registro de operaciones como medida técnica y organizativa, siendo las demás las que el responsable determine como las más adecuadas para lograr el control que se le solicita en virtud del tipo de tratamiento que se esté llevando a cabo y del nivel de riesgo que se estime, tras el correspondiente análisis. Se impone, asimismo, el deber de notificación a la autoridad de protección de datos de cualquier violación de la

seguridad que, con carácter general, deberá ser notificada al interesado, salvo en supuestos expresamente previstos en la ley.

El delegado de protección de datos se configura como el órgano o figura de asesoramiento y supervisión de los responsables de protección de datos, que podrá ser único para varias autoridades competentes y cuya designación será obligatoria salvo en relación con los tratamientos de datos con fines jurisdiccionales. En el caso de que se dispongan tratamientos que queden bajo distintos ámbitos de aplicación, con el fin de evitar disfunciones en las organizaciones de las autoridades competentes, se establece que la figura del delegado de protección de datos será única para todos ellos.

El capítulo V regula las transferencias de datos personales realizadas por las autoridades competentes españolas a un Estado que no sea miembro de la Unión Europea o a una organización internacional, incluidas las transferencias ulteriores a otro Estado que no pertenezca a la Unión Europea u otra organización internacional y se establecen las condiciones que deberán cumplirse para que estas sean lícitas.

Así, con el fin de garantizar que no se menoscabe el nivel de protección de las personas físicas previsto en esta Ley Orgánica, la transferencia respetará ciertas condiciones previstas en la misma. De este modo, sólo deben realizarse cuando sean necesarias para los fines de esta Ley Orgánica y cuando el responsable del tratamiento en el tercer país u organización internacional sea autoridad competente en relación a dichos fines.

Asimismo, cuando el dato se transfiere a un tercer país o a una organización internacional, la autoridad competente del Estado miembro en el que se obtuvo el dato, debe autorizar previamente esta transferencia y las ulteriores que puedan tener lugar a otro tercer país o a una organización internacional. En cuanto al tercer país u organización internacional destinatario de la trasferencia, deberá ser objeto de evaluación por la Comisión Europea a la vista de su nivel de protección de datos o, en caso de ausencia de decisión, debe entenderse por el responsable del tratamiento que ofrece garantías adecuadas. Sólo por las causas excepcionales previstas en esta Ley Orgánica se podrán autorizar transferencias fuera de estos supuestos. Este capítulo finaliza con la regulación de la transferencia internacional de datos personales a destinatarios que, no siendo autoridades competentes, están establecidos en terceros países.

El capítulo VI, relativo a las autoridades de protección de datos, dispone que dichas autoridades sean la Agencia Española de Protección de Datos y las Agencias Autonómicas de Protección de Datos, en sus respectivos ámbitos competenciales. Asimismo, la Ley Orgánica recoge sus potestades, funciones y la asistencia entre autoridades de protección de datos de los Estados miembros. Se remite en lo restante a la normativa que les resulte de aplicación.

El capítulo VII prevé que los procedimientos de reclamación que se planteen ante las autoridades de protección de datos se rijan por lo establecido en la Ley Orgánica 3/2018, de 5 de diciembre, o, en su caso, por la normativa reguladora de la autoridad de protección de datos correspondiente. Se refiere a aquellos supuestos en que los responsables o encargados del tratamiento, o de la autoridad de protección de datos, en su caso, incumplan esta Ley Orgánica y generen un daño o lesión en los bienes o derechos del interesado.

Este capítulo, además, aborda la responsabilidad de los responsables o encargados del tratamiento o de la autoridad de protección de datos, en su caso, cuando incumplan esta Ley Orgánica y se genere un daño o lesión en los bienes o derechos de un interesado. De igual modo, se detalla la forma de ejercer el derecho a la tutela judicial efectiva ante la jurisdicción contencioso-administrativa contra las decisiones de una autoridad de protección de datos que puedan entenderse que conciernen a los interesados.

Finalmente, el capítulo VIII regula el régimen sancionador específico aplicable ante incumplimientos de las obligaciones previstas en esta Ley Orgánica. Se definen los sujetos sobre los que recaerá la responsabilidad por las infracciones cometidas. Se determinan las reglas del concurso de normas para resolver los casos en los que un hecho pueda ser calificado con arreglo a dos o más de ellas, al tiempo que se tipifican las infracciones, que, en función de su gravedad, podrán ser leves, graves o muy graves. Por último, se establecen las sanciones que se pueden imponer, y se fijan los plazos de prescripción tanto de las infracciones como de las sanciones y de caducidad.

Las disposiciones adicionales se refieren a regímenes específicos, al intercambio de datos dentro de la Unión Europea, a los acuerdos internacionales en el ámbito de la cooperación judicial en materia penal y de la cooperación policial, y a los tratamientos que se efectúen en relación con los ficheros y al Registro de Población de las Administraciones Públicas.

Las disposiciones finales introducen las modificaciones necesarias en la Ley Orgánica 1/1979, de 26 de septiembre, General Penitenciaria, para adecuarla a las previsiones de esta Ley Orgánica en relación con los tratamientos para ejecución de la pena; en la Ley 50/1981, de 30 de diciembre; en la Ley Orgánica 6/1985, de 1 de julio; en la Ley Orgánica 3/2018, de 5 de diciembre; en la Ley Orgánica 1/2020, de 16 de septiembre, sobre la utilización de los datos del registro de nombres de pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves en correspondencia con determinadas obligaciones de los operadores; en la Ley 19/2007, de 11 de julio, contra la violencia, el racismo, la xenofobia y la intolerancia en el deporte; en la Ley 5/2014, de 4 de abril, de Seguridad Privada para adecuar, en ambos casos, los plazos de caducidad de los expedientes sancionadores; y en el texto refundido de la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial, aprobado por el Real Decreto Legislativo 6/2015, de 30 de octubre, para dar soporte legal específico a las matriculaciones por razones de Seguridad Nacional.

En la elaboración de esta Ley Orgánica se han observado los principios de necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia y eficiencia, exigidos por el artículo 129 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

En primer lugar, se trata de una norma necesaria, dado que la transposición de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, exige una ley de carácter orgánico, al afectar la norma comunitaria a un derecho fundamental reconocido en el artículo 18 de la Constitución y por imperativo del artículo 81 de la misma. En este sentido, el artículo 18.4 de la Constitución dispone que la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de la ciudadanía y el pleno ejercicio de sus derechos.

Esta Ley Orgánica, además, incorpora a nuestro ordenamiento interno los instrumentos que permitirán una eficaz protección de los datos de las personas físicas frente a su tratamiento por parte de las autoridades competentes con fines de prevención, detección, investigación o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública.

Por lo que respecta al principio de seguridad jurídica, en razón de la materia objeto de regulación, la transposición de la directiva se realiza mediante una Ley Orgánica, cuya tramitación e integración en el ordenamiento jurídico goza de las garantías que amparan las normas de esta naturaleza.

En cuanto al principio de proporcionalidad, esta Ley Orgánica contempla un importante número de garantías orientadas a que el tratamiento de datos personales sea proporcional, oportuno, mínimo y suficiente para el cumplimiento de los fines que se persiguen. En particular, su tratamiento se sujeta a los principios que rigen el tratamiento de datos personales, por lo que se exige que no sean tratados para otros fines distintos de los establecidos en la norma, salvo que dicho tratamiento esté autorizado por el Derecho de la Unión Europea o por nuestro Derecho interno. Cuando los datos personales sean tratados para otros fines que no sean los de la prevención, detección, investigación o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública, se aplicará el Reglamento General de Protección de Datos, a menos que el tratamiento se efectúe como parte de una actividad que quede fuera del ámbito de aplicación del Derecho de la Unión Europea.

Se cumple, también, el principio de transparencia, puesto que esta norma ha sido sometida a los correspondientes trámites de participación pública, esto es, el de consulta pública previa y el de audiencia e información pública.

En la tramitación de esta Ley Orgánica, además de los diversos Ministerios concernidos por razón de la materia, han emitido informe la Agencia Española de Protección de Datos; la Agencia Vasca de Protección de Datos; la Autoridad Catalana de Protección de Datos; el

Consejo Fiscal; el Consejo General del Poder Judicial; los Departamentos de Seguridad Pública del Gobierno Vasco y de Interior de la Generalidad de Cataluña; y finalmente el Consejo de Estado. Se trata, por tanto, de un texto en el cual se han incorporado las consideraciones de órganos tan relevantes como los expuestos.

Por último, esta Ley Orgánica se dicta al amparo de las reglas 1.ª, 6.ª, 18.ª y 29.ª del artículo 149.1 de la Constitución, que atribuyen al Estado las competencias exclusivas, respectivamente, para la regulación de las condiciones básicas que garanticen la igualdad de todos los españoles en el ejercicio de los derechos y en el cumplimiento de los deberes constitucionales; sobre legislación penal, penitenciaria y procesal; respecto a las bases del régimen jurídico de las Administraciones Públicas, el procedimiento administrativo común y en relación al sistema de responsabilidad de todas las Administraciones públicas; y en materia de seguridad pública.

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

Esta Ley Orgánica tiene por objeto establecer las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos de carácter personal por parte de las autoridades competentes, con fines de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública.

Artículo 2. *Ámbito de aplicación.*

1. Será de aplicación al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero, realizado por las autoridades competentes, con fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública.

2. El tratamiento de los datos personales llevado a cabo con ocasión de la tramitación por los órganos judiciales y fiscalías de las actuaciones o procesos de los que sean competentes, así como el realizado dentro de la gestión de la Oficina judicial y fiscal, en el ámbito del artículo 1, se regirá por lo dispuesto en la presente Ley Orgánica, sin perjuicio de las disposiciones de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, las leyes procesales que le sean aplicables y, en su caso, por la Ley 50/1981, de 30 de diciembre, por la que se regula el Estatuto Orgánico del Ministerio Fiscal. Las autoridades de protección de datos a las que se refiere el capítulo VI no serán competentes para controlar estas operaciones de tratamiento.

3. Quedan fuera del ámbito de aplicación de esta Ley Orgánica los siguientes tratamientos de datos personales:

a) Los realizados por las autoridades competentes para fines distintos de los previstos en el artículo 1, incluidos los fines de archivo por razones de interés público, investigación científica e histórica o estadísticos. Estos tratamientos se someterán plenamente a lo establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos), así como en la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales.

b) Los llevados a cabo por los órganos de la Administración General del Estado en el marco de las actividades comprendidas en el ámbito de aplicación del capítulo II del título V del Tratado de la Unión Europea.

c) Los tratamientos que afecten a actividades no comprendidas en el ámbito de aplicación del Derecho de la Unión Europea.

d) Los sometidos a la normativa sobre materias clasificadas, entre los que se encuentran los tratamientos relativos a la Defensa Nacional.

e) Los tratamientos realizados en las acciones civiles y procedimientos administrativos o de cualquier índole vinculados con los procesos penales que no tengan como objetivo directo ninguno de los fines del artículo 1.

4. Esta Ley Orgánica no se aplicará a los tratamientos de datos de personas fallecidas, sin perjuicio de lo establecido en el artículo siguiente.

Artículo 3. *Datos de personas fallecidas.*

1. Las personas vinculadas al fallecido por razones familiares o de hecho, así como sus herederos, podrán dirigirse al responsable o encargado del tratamiento al objeto de solicitar el acceso, rectificación o supresión de los datos de aquel. Estos derechos se regularán de acuerdo con lo dispuesto en esta Ley Orgánica.

2. En caso de fallecimiento de menores, estas facultades podrán ejercerse también por sus representantes legales o, en el marco de sus competencias, por el Ministerio Fiscal, que podrá actuar de oficio o a instancia de cualquier persona interesada.

3. En caso de fallecimiento de personas con discapacidad, estas facultades también podrán ejercerse, además de por quienes señala el apartado anterior, por quienes hubiesen sido designados para el ejercicio de funciones de apoyo, si tales facultades se entendieran comprendidas en las medidas de apoyo prestadas por el designado.

Artículo 4. *Autoridades competentes.*

1. Será autoridad competente, a los efectos de esta Ley Orgánica, toda autoridad pública que tenga competencias encomendadas legalmente para el tratamiento de datos personales con alguno de los fines previstos en el artículo 1.

En particular, tendrán esa consideración, en el ámbito de sus respectivas competencias, las siguientes autoridades:

a) Las Fuerzas y Cuerpos de Seguridad.

b) Las Administraciones Penitenciarias.

c) La Dirección Adjunta de Vigilancia Aduanera de la Agencia Estatal de Administración Tributaria.

d) El Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias.

e) La Comisión de Vigilancia de Actividades de Financiación del Terrorismo.

2. También tendrán consideración de autoridades competentes las Autoridades judiciales del orden jurisdiccional penal y el Ministerio Fiscal.

Artículo 5. *Definiciones.*

A efectos de esta Ley Orgánica se entenderá por:

a) «datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable a toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, unos datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;

b) «tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;

c) «limitación del tratamiento»: el marcado de los datos personales conservados con el fin de limitar su tratamiento en el futuro;

d) «elaboración de perfiles»: toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física;

e) «seudonimización»: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional se mantenga por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable;

f) «fichero»: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o dispersado de forma funcional o geográfica;

g) «responsable del tratamiento» o «responsable»: la autoridad competente que sola o conjuntamente con otras, determine los fines y medios del tratamiento de datos personales; en caso de que los fines y medios del tratamiento estén determinados por el Derecho de la Unión Europea o por la legislación española, dichas normas podrán designar al responsable del tratamiento, o bien los criterios para su nombramiento.

h) «encargado del tratamiento» o «encargado»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;

i) «destinatario»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerará destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con la legislación española o de la Unión Europea; el tratamiento de tales datos por las citadas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento;

j) «violación de la seguridad de los datos personales»: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita, o la comunicación o acceso no autorizados a datos personales transmitidos, conservados o tratados de otra forma;

k) «datos genéticos»: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de la persona física de que se trate;

l) «datos biométricos»: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o de conducta de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos;

m) «datos relativos a la salud»: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud;

n) «organización internacional»: una organización internacional y sus entes subordinados de Derecho internacional público o cualquier otro organismo creado mediante un acuerdo entre dos o más países o en virtud de tal acuerdo.

CAPÍTULO II

Principios, licitud del tratamiento y videovigilancia

Sección 1.ª Principios y licitud del tratamiento

Artículo 6. *Principios relativos al tratamiento de datos personales.*

1. Los datos personales serán:

a) Tratados de manera lícita y leal.

b) Recogidos con fines determinados, explícitos y legítimos, y no serán tratados de forma incompatible con esos fines.

c) Adecuados, pertinentes y no excesivos en relación con los fines para los que son tratados.

d) Exactos y, si fuera necesario, actualizados. Se adoptarán todas las medidas razonables para que se supriman o rectifiquen, sin dilación indebida, los datos personales que sean inexactos con respecto a los fines para los que son tratados.

e) Conservados de forma que permitan identificar al interesado durante un período no superior al necesario para los fines para los que son tratados.

f) Tratados de manera que se garantice una seguridad adecuada, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental. Para ello, se utilizarán las medidas técnicas u organizativas adecuadas.

2. Los datos personales recogidos por las autoridades competentes no serán tratados para otros fines distintos de los establecidos en el artículo 1, salvo que dicho tratamiento esté autorizado por el Derecho de la Unión Europea o por la legislación española. Cuando los datos personales sean tratados para otros fines, se aplicará el Reglamento General de Protección de Datos y la Ley Orgánica 3/2018, de 5 de diciembre, a menos que el tratamiento se efectúe como parte de una actividad que quede fuera del ámbito de aplicación del Derecho de la Unión Europea.

3. Los datos personales podrán ser tratados por el mismo responsable o por otro, para fines establecidos en el artículo 1 distintos de aquel para el que hayan sido recogidos, en la medida en que concurran cumulativamente las dos circunstancias siguientes:

a) Que el responsable del tratamiento sea competente para tratar los datos para ese otro fin, de acuerdo con el Derecho de la Unión Europea o la legislación española.

b) Que el tratamiento sea necesario y proporcionado para la consecución de ese otro fin, de acuerdo con el Derecho de la Unión Europea o la legislación española.

4. El tratamiento por el mismo responsable o por otro podrá incluir el archivo por razones de interés público, y el uso científico, estadístico o histórico para los fines establecidos en el artículo 1, con sujeción a las garantías adecuadas para los derechos y libertades de los interesados.

5. El responsable del tratamiento deberá garantizar y estar en condiciones de demostrar el cumplimiento de lo establecido en este artículo.

Artículo 7. *Deber de colaboración.*

1. Las Administraciones públicas, así como cualquier persona física o jurídica, proporcionarán a las autoridades judiciales, al Ministerio Fiscal o a la Policía Judicial los datos, informes, antecedentes y justificantes que les soliciten y que sean necesarios para la investigación y enjuiciamiento de infracciones penales o para la ejecución de las penas. La petición de la Policía Judicial se deberá ajustar exclusivamente al ejercicio de las funciones que le encomienda el artículo 549.1 de la Ley Orgánica 6/1985, de 1 de julio y deberá efectuarse siempre de forma motivada, concreta y específica, dando cuenta en todo caso a la autoridad judicial y fiscal.

La comunicación de datos, informes, antecedentes y justificantes por la Administración Tributaria, la Administración de la Seguridad Social y la Inspección de Trabajo y Seguridad Social, se efectuará de acuerdo con su legislación respectiva.

2. En los restantes casos, las Administraciones públicas, así como cualquier persona física o jurídica, proporcionarán los datos, informes, antecedentes y justificantes a las autoridades competentes que los soliciten, siempre que estos sean necesarios para el desarrollo específico de sus misiones para la prevención, detección e investigación de infracciones penales y para la prevención y protección frente a un peligro real y grave para la seguridad pública. La petición de la autoridad competente deberá ser concreta y específica y contener la motivación que acredite su relación con los indicados supuestos.

3. No será de aplicación lo dispuesto en los apartados anteriores cuando legalmente sea exigible la autorización judicial para recabar los datos necesarios para el cumplimiento de los fines del artículo 1.

4. En los supuestos contemplados en los apartados anteriores, el interesado no será informado de la transmisión de sus datos a las autoridades competentes, ni de haber

facilitado el acceso a los mismos por dichas autoridades de cualquier otra forma, a fin de garantizar la actividad investigadora.

Con el mismo propósito, los sujetos a los que el ordenamiento jurídico imponga un deber específico de colaboración con las autoridades competentes para el cumplimiento de los fines establecidos en el artículo 1, no informarán al interesado de la transmisión de sus datos a dichas autoridades, ni de haber facilitado el acceso a los mismos por dichas autoridades de cualquier otra forma, en cumplimiento de sus obligaciones específicas.

Artículo 8. *Plazos de conservación y revisión.*

1. El responsable del tratamiento determinará que la conservación de los datos personales tenga lugar sólo durante el tiempo necesario para cumplir con los fines previstos en el artículo 1.
2. El responsable del tratamiento deberá revisar la necesidad de conservar, limitar o suprimir el conjunto de los datos personales contenidos en cada una de las actividades de tratamiento bajo su responsabilidad, como máximo cada tres años, atendiendo especialmente en cada revisión a la edad del afectado, el carácter de los datos y a la conclusión de una investigación o procedimiento penal. Si es posible, se hará mediante el tratamiento automatizado apropiado.
3. Con carácter general, el plazo máximo para la supresión de los datos será de veinte años, salvo que concurran factores como la existencia de investigaciones abiertas o delitos que no hayan prescrito, la no conclusión de la ejecución de la pena, reincidencia, necesidad de protección de las víctimas u otras circunstancias motivadas que hagan necesario el tratamiento de los datos para el cumplimiento de los fines del artículo 1.

Artículo 9. *Distinción entre categorías de interesados.*

El responsable del tratamiento, en la medida de lo posible, establecerá entre los datos personales de las distintas categorías de interesados, distinciones tales como:

a) Personas respecto de las cuales existan motivos fundados para presumir que hayan cometido, puedan cometer o colaborar en la comisión de una infracción penal.
b) Personas condenadas o sancionadas por una infracción penal.
c) Víctimas o afectados por una infracción penal o que puedan serlo.
d) Terceros involucrados en una infracción penal como son: personas que puedan ser citadas a testificar en investigaciones relacionadas con infracciones o procesos penales ulteriores, personas que puedan facilitar información sobre dichas infracciones, o personas de contacto o asociados de una de las personas mencionadas en las letras a) y b).

Lo anterior no debe impedir la aplicación del derecho a la presunción de inocencia tal como lo garantiza el artículo 24 de la Constitución.

Artículo 10. *Verificación de la calidad de los datos personales.*

1. El responsable del tratamiento, en la medida de lo posible, establecerá una distinción entre los datos personales basados en hechos y los basados en apreciaciones personales.
2. Las autoridades competentes adoptarán todas las medidas razonables para garantizar que los datos personales que sean inexactos, incompletos o no estén actualizados, no se transmitan ni se pongan a disposición de terceros. En toda transmisión de datos se trasladará al mismo tiempo la valoración de su calidad, exactitud y actualización.
En la medida de lo posible, en todas las transmisiones de datos personales se añadirá la información necesaria para que la autoridad competente receptora pueda valorar hasta qué punto son exactos, completos y fiables, y en qué medida están actualizados. Igualmente, la autoridad competente transmisora, en la medida en que sea factible, controlará la calidad de los datos personales antes de transmitirlos o ponerlos a disposición de terceros.
3. Si se observara que los datos personales transmitidos son incorrectos o que se han transmitido ilegalmente, estas circunstancias se pondrán en conocimiento del destinatario sin dilación indebida. En tal caso, los datos deberán rectificarse o suprimirse, o el tratamiento deberá limitarse de conformidad con lo previsto en el artículo 23.

Artículo 11. *Licitud del tratamiento.*

1. El tratamiento sólo será lícito en la medida en que sea necesario para los fines señalados en el artículo 1 y se realice por una autoridad competente en ejercicio de sus funciones.

2. Cualquier ley que regule tratamientos de datos personales para los fines incluidos dentro del ámbito de aplicación de esta Ley Orgánica deberá indicar, al menos, los objetivos del tratamiento, los datos personales que vayan a ser objeto del mismo y las finalidades del tratamiento.

Artículo 12. *Condiciones específicas de tratamiento.*

1. Cuando el Derecho de la Unión Europea o la legislación española prevea condiciones específicas aplicables al tratamiento, la autoridad competente transmitente deberá informar al destinatario al que se transmitan los datos, de dichas condiciones y de la obligación de respetarlas.

2. Las condiciones específicas de tratamiento podrán ser, entre otras, la prohibición de transmisión de datos o de su utilización para fines distintos para los que fueron transmitidos o, en caso de limitación del derecho a la información, la prohibición de dar información al interesado sin la autorización previa de la autoridad transmisora.

3. La autoridad competente transmitente no aplicará a los destinatarios de otros Estados miembros de la Unión Europea o de organismos, agencias y órganos establecidos en virtud de los capítulos 4 y 5 del título V de la tercera parte del Tratado de Funcionamiento de la Unión Europea, condiciones distintas de las aplicables a las transmisiones de datos similares dentro de España.

Artículo 13. *Tratamiento de categorías especiales de datos personales.*

1. El tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas o la afiliación sindical, así como el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, los datos relativos a la salud o a la vida sexual o a la orientación sexual de una persona física, sólo se permitirá cuando sea estrictamente necesario, con sujeción a las garantías adecuadas para los derechos y libertades del interesado y cuando se cumplan alguna de las siguientes circunstancias:

a) Se encuentre previsto por una norma con rango de ley o por el Derecho de la Unión Europea.

b) Resulte necesario para proteger los intereses vitales, así como los derechos y libertades fundamentales del interesado o de otra persona física.

c) Dicho tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos.

2. Las autoridades competentes, en el marco de sus respectivas funciones y competencias, podrán tratar datos biométricos dirigidos a identificar de manera unívoca a una persona física con los fines de prevención, investigación, detección de infracciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública.

3. Los datos de los menores de edad y de las personas con capacidad modificada judicialmente o que estén incursas en procesos de dicha naturaleza, se tratarán garantizando el interés superior de los mismos y con el nivel de seguridad adecuado.

Artículo 14. *Mecanismo de decisión individual automatizado.*

1. Están prohibidas las decisiones basadas únicamente en un tratamiento automatizado, incluida la elaboración de perfiles, que produzcan efectos jurídicos negativos para el interesado o que le afecten significativamente, salvo que se autorice expresamente por una norma con rango de ley o por el Derecho de la Unión Europea. La norma habilitante del tratamiento deberá establecer las medidas adecuadas para salvaguardar los derechos y libertades del interesado, incluyendo el derecho a obtener la intervención humana en el proceso de revisión de la decisión adoptada.

2. Las decisiones a las que se refiere el apartado anterior no se basarán en las categorías especiales de datos personales contempladas en el artículo 13, salvo que se hayan tomado las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.

3. Queda prohibida la elaboración de perfiles que dé lugar a una discriminación de las personas físicas sobre la base de categorías especiales de datos personales establecidas en el artículo 13.

Sección 2.ª Tratamiento de datos personales en el ámbito de la videovigilancia por Fuerzas y Cuerpos de Seguridad

Artículo 15. *Sistemas de grabación de imágenes y sonido por las Fuerzas y Cuerpos de Seguridad.*

1. La captación, reproducción y tratamiento de datos personales por las Fuerzas y Cuerpos de Seguridad en los términos previstos en esta Ley Orgánica, así como las actividades preparatorias, no se considerarán intromisiones ilegítimas en el derecho al honor, a la intimidad personal y familiar y a la propia imagen, a los efectos de lo establecido en el artículo 2.2 de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

2. En la instalación de sistemas de grabación de imágenes y sonidos se tendrán en cuenta, conforme al principio de proporcionalidad, los siguientes criterios: asegurar la protección de los edificios e instalaciones propias; asegurar la protección de edificios e instalaciones públicas y de sus accesos que estén bajo custodia; salvaguardar y proteger las instalaciones útiles para la seguridad nacional y prevenir, detectar o investigar la comisión de infracciones penales y la protección y prevención frente a las amenazas contra la seguridad pública.

Artículo 16. *Instalación de sistemas fijos.*

1. En las vías o lugares públicos donde se instalen videocámaras fijas, el responsable del tratamiento deberá realizar una valoración del citado principio de proporcionalidad en su doble versión de idoneidad e intervención mínima. Asimismo, deberá llevar a cabo un análisis de los riesgos o una evaluación de impacto de protección de datos relativo al tratamiento que se pretenda realizar, en función del nivel de perjuicio que se pueda derivar para la ciudadanía y de la finalidad perseguida.

Se entenderá por videocámara fija aquella anclada a un soporte fijo o fachada, aunque el sistema de grabación se pueda mover en cualquier dirección.

2. Esta disposición se aplicará asimismo cuando las Fuerzas y Cuerpos de Seguridad utilicen instalaciones fijas de videocámaras de las que no sean titulares y exista, por su parte, un control y dirección efectiva del proceso completo de tratamiento.

3. Estas instalaciones fijas de videocámaras no estarán sujetas al control preventivo de las entidades locales previsto en su legislación reguladora básica, ni al ejercicio de las competencias de las diferentes Administraciones públicas, sin perjuicio de que deban respetar los principios de la legislación vigente en cada ámbito material de la actuación administrativa.

4. Los propietarios y, en su caso, los titulares de derechos reales sobre los bienes afectados por estas instalaciones, o quienes los posean por cualquier título, están obligados a facilitar y permitir su instalación y mantenimiento, sin perjuicio de las indemnizaciones que procedan.

5. Los ciudadanos serán informados de manera clara y permanente de la existencia de estas videocámaras fijas, sin especificar su emplazamiento, así como de la autoridad responsable del tratamiento ante la que poder ejercer sus derechos.

Artículo 17. *Dispositivos móviles.*

1. Podrán utilizarse dispositivos de toma de imágenes y sonido de carácter móvil para el mejor cumplimiento de los fines previstos en esta Ley Orgánica, conforme a las competencias específicas de las Fuerzas y Cuerpos de Seguridad. La toma de imagen y

sonido, que ha de ser conjunta, queda supeditada, en todo caso, a la concurrencia de un peligro o evento concreto. El uso de los dispositivos móviles deberá estar autorizado por la persona titular de la Delegación o Subdelegación del Gobierno, quien atenderá a la naturaleza de los eventuales hechos susceptibles de filmación, adecuando la utilización de dichos dispositivos a los principios de tratamiento y al de proporcionalidad.

En el caso de los Cuerpos de Policía propios de las Comunidades Autónomas que tengan y ejerzan competencias asumidas para la protección de las personas y bienes y para el mantenimiento del orden público, serán sus órganos correspondientes los que autorizarán este tipo de actuaciones para sus fuerzas policiales, así como para las dependientes de las Corporaciones locales radicadas en su territorio.

2. En estos supuestos de dispositivos móviles, las autorizaciones no se podrán conceder en ningún caso con carácter indefinido o permanente, siendo otorgadas por el plazo adecuado a la naturaleza y las circunstancias derivadas del peligro o evento concreto, por un periodo máximo de un mes prorrogable por otro.

3. En casos de urgencia o necesidad inaplazable será el responsable operativo de las Fuerzas y Cuerpos de Seguridad competentes el que podrá determinar su uso, siendo comunicada tal actuación con la mayor brevedad posible, y siempre en el plazo de 24 horas, al Delegado o Subdelegado del Gobierno o autoridad competente de las comunidades autónomas.

Artículo 18. *Tratamiento y conservación de las imágenes.*

1. Realizada la filmación de acuerdo con los requisitos establecidos en esta Ley Orgánica, si la grabación captara la comisión de hechos que pudieran ser constitutivos de infracciones penales, las Fuerzas y Cuerpos de Seguridad pondrán la cinta o soporte original de las imágenes y sonidos en su integridad, a disposición judicial a la mayor brevedad posible y, en todo caso, en el plazo máximo de setenta y dos horas desde su grabación. De no poder redactarse el atestado en tal plazo, se relatarán verbalmente los hechos a la autoridad judicial, o al Ministerio Fiscal, junto con la entrega de la grabación.

2. Si se captaran hechos que pudieran ser constitutivos de infracciones administrativas relacionadas con la seguridad pública, se remitirán al órgano competente, de inmediato, para el inicio del oportuno procedimiento sancionador.

3. Las grabaciones serán destruidas en el plazo máximo de tres meses desde su captación, salvo que estén relacionadas con infracciones penales o administrativas graves o muy graves en materia de seguridad pública, sujetas a una investigación policial en curso o con un procedimiento judicial o administrativo abierto.

Artículo 19. *Régimen disciplinario.*

1. Sin perjuicio de las responsabilidades penales en las que pudieran incurrir, las infracciones a lo dispuesto en esta Ley Orgánica por los miembros de las Fuerzas y Cuerpos de Seguridad, serán sancionadas con arreglo al régimen disciplinario correspondiente a los infractores y, en su defecto, con sujeción al régimen general de sanciones en materia de protección de datos de carácter personal establecido en esta Ley Orgánica.

2. Se considerarán faltas muy graves en el régimen disciplinario de las Fuerzas y Cuerpos de Seguridad del Estado, las siguientes infracciones:

a) Alterar o manipular los registros de imágenes y sonidos, siempre que no constituya delito.

b) Permitir el acceso de personas no autorizadas a las imágenes y sonidos grabados o utilizar estos para fines distintos de los previstos legalmente.

c) Reproducir las imágenes y sonidos para fines distintos de los previstos en esta Ley Orgánica.

d) Utilizar los medios técnicos regulados en esta Ley Orgánica para fines distintos de los previstos en la misma.

CAPÍTULO III

Derechos de las personas

Sección 1.ª Régimen general

Artículo 20. *Condiciones generales de ejercicio de los derechos de los interesados.*

1. El responsable del tratamiento deberá facilitar al interesado, de forma concisa, inteligible, de fácil acceso y con lenguaje claro y sencillo para todas las personas, incluidas aquellas con discapacidad, toda la información contemplada en el artículo 21, así como la derivada de los artículos 14, 22 a 26 y 39.

Además, el responsable del tratamiento deberá adoptar las medidas necesarias para garantizar al interesado el ejercicio de sus derechos a los que se refieren los artículos 14 y 22 a 26.

2. El interesado, con capacidad de obrar, podrá actuar en su propio nombre y representación o por medio de representantes, de acuerdo con lo previsto en la normativa sobre el procedimiento administrativo común de las Administraciones Públicas.

3. La información será facilitada por cualquier medio adecuado, incluidos los medios electrónicos, procurando utilizar el mismo medio empleado en la solicitud.

4. El responsable del tratamiento informará por escrito al interesado, sin dilación indebida, sobre el curso dado a su solicitud. La solicitud se entenderá desestimada si transcurrido un mes desde su presentación no ha sido resuelta expresamente y notificada al interesado.

5. La información a la que se refiere el apartado 1 se facilitará gratuitamente. Cuando las solicitudes de un interesado sean manifiestamente infundadas o excesivas, en particular debido a su carácter repetitivo, el responsable del tratamiento podrá inadmitirlas a trámite, mediante resolución motivada.

El responsable del tratamiento deberá demostrar el carácter manifiestamente infundado o excesivo de la solicitud.

En todo caso se considerará que la solicitud es repetitiva cuando se realicen tres solicitudes sobre el mismo supuesto durante el plazo de seis meses, salvo que exista causa legítima para ello.

6. Cuando el responsable del tratamiento tenga dudas razonables acerca de la identidad de la persona física que formula la solicitud a la que se refieren los artículos 22 y 23, le requerirá para que facilite la información complementaria que resulte necesaria para confirmar su identidad en el plazo de diez días. Transcurrido dicho plazo sin que se aporte la información, se le tendrá por desistido de su petición mediante resolución motivada. El plazo al que se refiere el apartado 4 comenzará a computarse desde la fecha en la que se facilite dicha información complementaria.

Artículo 21. *Información que debe ponerse a disposición del interesado.*

1. El responsable del tratamiento de los datos pondrá a disposición del interesado, al menos, la siguiente información:

a) La identificación del responsable del tratamiento y sus datos de contacto.

b) Los datos de contacto del delegado de protección de datos, en su caso.

c) Los fines del tratamiento a los que se destinen los datos personales.

d) El derecho a presentar una reclamación ante la autoridad de protección de datos competente y los datos de contacto de la misma.

e) El derecho a solicitar del responsable del tratamiento el acceso a los datos personales relativos al interesado y su rectificación, supresión o la limitación de su tratamiento.

2. Además de la información a la que se refiere el apartado 1, atendiendo a las circunstancias del caso concreto, el responsable del tratamiento proporcionará al interesado la siguiente información adicional para permitir el ejercicio de sus derechos:

a) La base jurídica del tratamiento.

b) El plazo durante el cual se conservarán los datos personales o, cuando esto no sea posible, los criterios utilizados para determinar ese plazo.

c) Las categorías de destinatarios de los datos personales, cuando corresponda, en particular, los establecidos en Estados que no sean miembros de la Unión Europea u organizaciones internacionales.

d) Cualquier otra información necesaria, en especial, cuando los datos personales se hayan recogido sin conocimiento del interesado.

Artículo 22. *Derecho de acceso del interesado a sus datos personales.*

1. El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen. En caso de que se confirme el tratamiento, el interesado tendrá derecho a acceder a dichos datos personales, así como a la siguiente información:

a) Los fines y la base jurídica del tratamiento.

b) Las categorías de datos personales de que se trate.

c) Los destinatarios o las categorías de destinatarios a quienes hayan sido comunicados los datos personales, en particular, los destinatarios establecidos en Estados que no sean miembros de la Unión Europea u organizaciones internacionales.

d) El plazo de conservación de los datos personales, cuando sea posible, o, en caso contrario, los criterios utilizados para determinar dicho plazo.

e) La existencia del derecho a solicitar del responsable del tratamiento la rectificación o supresión de los datos personales relativos al interesado o la limitación de su tratamiento.

f) El derecho a presentar una reclamación ante la autoridad de protección de datos competente y los datos de contacto de la misma.

g) La comunicación de los datos personales objeto de tratamiento, así como cualquier información disponible sobre su origen, sin revelar la identidad de ninguna persona física, en especial en el caso de fuentes confidenciales.

2. Cuando el responsable trate una gran cantidad de información relativa al interesado y éste ejercite su derecho de acceso sin especificar si se refiere a todos o a una parte de los datos, el responsable podrá requerir al interesado que concrete la solicitud en el plazo de diez días.

3. Se entenderá concedido el derecho de acceso si el responsable del tratamiento facilita al interesado un sistema remoto, directo y seguro que garantice, de modo permanente, el acceso a la totalidad de sus datos personales. La notificación informando al interesado del procedimiento puesto en marcha a través de este sistema, permitirá denegar su solicitud de acceso efectuada por otras vías.

Si el acceso remoto no facilita la totalidad de la información contenida en el apartado 1, el interesado tendrá derecho a solicitarla.

4. Cuando el interesado elija un medio distinto al que se le ofrece que suponga un coste desproporcionado, la solicitud será considerada excesiva, por lo que dicho interesado asumirá el exceso de coste que su elección comporte. En este caso, sólo será exigible al responsable del tratamiento que la satisfacción del derecho de acceso a través del medio propuesto se produzca sin dilaciones indebidas. Si el interesado no asumiera el exceso de coste, se le facilitará el acceso por el medio inicialmente propuesto por el responsable del tratamiento.

Artículo 23. *Derechos de rectificación, supresión de datos personales y limitación de su tratamiento.*

1. El interesado tendrá derecho a obtener del responsable del tratamiento, sin dilación indebida, la rectificación de los datos personales que le conciernen, cuando tales datos resulten inexactos.

Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales cuando estos resulten incompletos.

El interesado deberá indicar en su solicitud a qué datos se refiere y la corrección que haya de realizarse. Deberá acompañar, cuando sea preciso, la documentación justificativa del carácter incompleto o inexacto de los datos objeto de tratamiento.

2. El responsable del tratamiento, a iniciativa propia o como consecuencia del ejercicio del derecho de supresión del interesado, suprimirá los datos personales sin dilación indebida

y, en todo caso, en el plazo máximo de un mes a contar desde que tenga conocimiento, cuando el tratamiento infrinja los artículos 6, 11 o 13, o cuando los datos personales deban ser suprimidos en virtud de una obligación legal a la que esté sujeto.

3. En lugar de proceder a la supresión, el responsable del tratamiento limitará el tratamiento de los datos personales cuando se dé alguna de las siguientes circunstancias:

a) El interesado ponga en duda la exactitud de los datos personales y no pueda determinarse su exactitud o inexactitud.

b) Los datos personales hayan de conservarse a efectos probatorios.

Cuando el tratamiento esté limitado en virtud de la letra a), el responsable del tratamiento informará al interesado antes de levantar la limitación del tratamiento.

4. En caso de que el responsable del tratamiento rectifique unos datos personales inexactos que provengan de otra autoridad competente, se deberá comunicar a esta la rectificación.

5. Cuando los datos personales hayan sido rectificados o suprimidos o el tratamiento haya sido limitado, el responsable del tratamiento lo notificará a los destinatarios, que deberán rectificar o suprimir los datos personales que estén bajo su responsabilidad o limitar su tratamiento.

Artículo 24. *Restricciones a los derechos de información, acceso, rectificación, supresión de datos personales y a la limitación de su tratamiento.*

1. El responsable del tratamiento podrá aplazar, limitar u omitir la información a la que se refiere el artículo 21.2, así como denegar, total o parcialmente, las solicitudes de ejercicio de los derechos contemplados en los artículos 22 y 23, siempre que, teniendo en cuenta los derechos fundamentales y los intereses legítimos de la persona afectada, resulte necesario y proporcional para la consecución de los siguientes fines:

a) Impedir que se obstaculicen indagaciones, investigaciones o procedimientos judiciales.

b) Evitar que se cause perjuicio a la prevención, detección, investigación y enjuiciamiento de infracciones penales o a la ejecución de sanciones penales.

c) Proteger la seguridad pública.

d) Proteger la Seguridad Nacional.

e) Proteger los derechos y libertades de otras personas.

2. En caso de restricción de los derechos contemplados en los artículos 22 y 23, el responsable del tratamiento informará por escrito al interesado sin dilación indebida, y en todo caso, en el plazo de un mes a contar desde que tenga conocimiento, de dicha restricción, de las razones de la misma, así como de las posibilidades de presentar una reclamación ante la autoridad de protección de datos, sin perjuicio de las restantes acciones judiciales que pueda ejercer en virtud de lo dispuesto en esta Ley Orgánica.

Las razones de la restricción podrán ser omitidas o ser sustituidas por una redacción neutra cuando la revelación de los motivos de la restricción pueda poner en riesgo los fines a los que se refiere el apartado anterior.

3. El responsable del tratamiento documentará los fundamentos de hecho o de derecho en los que se sustente la decisión denegatoria del ejercicio del derecho de acceso. Dicha información estará a disposición de las autoridades de protección de datos.

Artículo 25. *Ejercicio de los derechos del interesado a través de la autoridad de protección de datos.*

1. En los casos en que se produzca un aplazamiento, limitación u omisión de la información a que se refiere el artículo 21 o una restricción del ejercicio de los derechos contemplados en los artículos 22 y 23, en los términos previstos en el artículo 24, el interesado podrá ejercer sus derechos a través de la autoridad de protección de datos competente. El responsable del tratamiento informará al interesado de esta posibilidad.

2. Cuando, en virtud de lo establecido en el apartado anterior, se ejerciten los derechos a través de la autoridad de protección de datos, esta deberá informar al interesado, al menos,

de la realización de todas las comprobaciones necesarias o la revisión correspondiente y de su derecho a interponer recurso contencioso-administrativo.

Sección 2.ª Régimen especial

Artículo 26. *Derechos de los interesados como consecuencia de investigaciones y procesos penales.*

1. El ejercicio de los derechos de información, acceso, rectificación, supresión y limitación del tratamiento a los que se hace referencia en los artículos anteriores se llevará a cabo de conformidad con las normas procesales penales cuando los datos personales figuren en una resolución judicial, o en un registro, diligencias o expedientes tramitados en el curso de investigaciones y procesos penales.

2. Cuando los datos sean objeto de un tratamiento con fines jurisdiccionales del que sea responsable un órgano del orden jurisdiccional penal, o el Ministerio Fiscal, el ejercicio de los derechos de información, acceso, rectificación, supresión y limitación del tratamiento se realizará de conformidad con lo previsto en la Ley Orgánica 6/1985, de 1 de julio, en las normas procesales y en su caso, el Estatuto Orgánico del Ministerio Fiscal.

3. En defecto de regulación del ejercicio de estos derechos en dichas normas, se aplicará lo dispuesto en esta Ley Orgánica.

CAPÍTULO IV

Responsable y encargado de tratamiento

Sección 1.ª Obligaciones generales

Artículo 27. *Obligaciones del responsable del tratamiento.*

1. El responsable del tratamiento, tomando en consideración la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los niveles de riesgo para los derechos y libertades de las personas físicas, aplicará las medidas técnicas y organizativas apropiadas para garantizar que el tratamiento se lleve a cabo de acuerdo con esta Ley Orgánica y con lo previsto en la legislación sectorial y en sus normas de desarrollo. Tales medidas se revisarán y actualizarán cuando resulte necesario.

2. Entre las medidas mencionadas en el apartado anterior se incluirá la aplicación de las oportunas políticas de protección de datos, cuando sean proporcionadas en relación con las actividades de tratamiento.

Artículo 28. *Protección de datos desde el diseño y por defecto.*

1. En el momento de determinar los medios para el tratamiento, así como en el momento del tratamiento propiamente dicho, deberán aplicarse las medidas técnicas y organizativas que resulten apropiadas conforme al estado de la técnica y el coste de la aplicación, la naturaleza, el ámbito, el contexto, los fines del tratamiento y los riesgos para los derechos y libertades de las personas físicas. El objetivo será salvaguardar los principios de protección de datos de forma efectiva, al tiempo que integrar las garantías necesarias en el tratamiento. Entre estas medidas técnicas, se podrá adoptar la seudonimización de los datos personales a los efectos de contribuir a la aplicación de los principios establecidos en esta Ley Orgánica, en particular, el de minimización de datos personales.

2. Además, las medidas técnicas y organizativas deberán garantizar que, por defecto, sólo sean objeto de tratamiento los datos personales que resulten necesarios para cada uno de los fines específicos del tratamiento. Dicha obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su período de conservación y a su accesibilidad.

Tales medidas garantizarán que, por defecto, los datos personales no sean accesibles a un número indeterminado de personas sin intervención humana.

Artículo 29. *Supuestos de corresponsabilidad en el tratamiento.*

1. Cuando dos o más responsables del tratamiento determinen conjuntamente los objetivos y los medios de tratamiento serán considerados corresponsables del tratamiento.

2. Salvo que las responsabilidades hayan sido previstas por el Derecho de la Unión Europea o por la legislación española, los corresponsables del tratamiento establecerán, de modo transparente y de mutuo acuerdo, a través del instrumento oportuno, sus respectivas responsabilidades en el cumplimiento de esta Ley Orgánica, en particular, en lo referido al ejercicio de los derechos del interesado y a sus respectivas obligaciones en el suministro de la información contemplada en el artículo 21.

El citado acuerdo designará el punto de contacto para los interesados, a menos que venga ya determinado legalmente.

La concreción de las responsabilidades se realizará atendiendo a las actividades que efectivamente desarrolle cada uno de los corresponsables del tratamiento.

Artículo 30. *Encargado del tratamiento.*

1. Cuando una operación de tratamiento vaya a ser llevada a cabo por cuenta de un responsable del tratamiento, este recurrirá únicamente a encargados que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos de esta Ley Orgánica y garantice la protección de los derechos del interesado.

El encargado podrá ser una persona física o jurídica, de naturaleza privada o pública.

2. El encargado del tratamiento no recurrirá a otro encargado sin la autorización previa por escrito del responsable del tratamiento. El encargado informará siempre al responsable de cualquier cambio previsto referido a la adición o sustitución de otros encargados, pudiendo el responsable oponerse a dichos cambios.

3. El tratamiento por medio de un encargado se regirá por un contrato, convenio u otro instrumento jurídico que corresponda, por escrito, incluyendo la posibilidad del formato electrónico, concluido con arreglo al Derecho de la Unión Europea o a la legislación española. Dicho instrumento jurídico vinculará al encargado con el responsable y fijará el objeto y la duración del tratamiento, su naturaleza y finalidad, el tipo de datos personales y categorías de interesados, así como las obligaciones y derechos del responsable.

El instrumento jurídico estipulará, en particular, que el encargado del tratamiento deberá:

a) Actuar únicamente siguiendo las instrucciones del responsable del tratamiento.

b) Garantizar, a través del instrumento o sistema oportuno, que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación profesional de secreto o confidencialidad.

c) Asistir al responsable del tratamiento por cualquier medio adecuado para garantizar el cumplimiento de las disposiciones sobre los derechos del interesado.

d) Suprimir o devolver, a elección del responsable del tratamiento, todos los datos personales al responsable del tratamiento, una vez finalice la prestación de los servicios de tratamiento, así como suprimir las copias existentes, a menos que el Derecho de la Unión Europea o la legislación española requieran la conservación de los datos personales.

e) Poner a disposición del responsable del tratamiento toda la información necesaria para demostrar el cumplimiento de estas obligaciones.

f) Respetar las condiciones indicadas en este apartado y en el apartado 2 para contratar a otro encargado del tratamiento.

4. Si un encargado del tratamiento determinase los fines y medios de dicho tratamiento, infringiendo esta Ley Orgánica, será considerado responsable con respecto a ese tratamiento.

5. El encargado del tratamiento se regirá, en lo no previsto por esta Ley Orgánica, por lo establecido en la Ley Orgánica 3/2018, de 5 de diciembre.

Artículo 31. *Tratamiento bajo la autoridad del responsable o del encargado del tratamiento.*

El encargado del tratamiento, así como cualquier persona que actúe bajo la autoridad del responsable o del encargado del tratamiento y tenga acceso a datos personales, sólo podrá

someterlos a tratamiento siguiendo instrucciones del responsable del tratamiento, a menos que esté obligado a hacerlo por el Derecho de la Unión Europea o por la legislación española.

Artículo 32. *Registros de las actividades de tratamiento.*

1. Cada responsable debe conservar un registro de todas las actividades de tratamiento de datos personales efectuadas bajo su responsabilidad. Dicho registro deberá contener la información siguiente:

a) La identificación del responsable del tratamiento y sus datos de contacto, así como, en su caso, del corresponsable y del delegado de protección de datos.
b) Los fines del tratamiento.
c) Las categorías de destinatarios a quienes se hayan comunicado o vayan a comunicarse los datos personales, incluidos los destinatarios en Estados que no sean miembros de la Unión Europea u organizaciones internacionales.
d) La descripción de las categorías de interesados y de las categorías de datos personales.
e) El recurso a la elaboración de perfiles, en su caso.
f) Las categorías de transferencias de datos personales a un Estado que no sea miembro de la Unión Europea o a una organización internacional, en su caso.
g) La indicación de la base jurídica del tratamiento, así como, en su caso, las transferencias internacionales de las que van a ser objeto los datos personales.
h) Los plazos previstos para la supresión de las diferentes categorías de datos personales, cuando sea posible.
i) La descripción general de las medidas técnicas y organizativas de seguridad a las que se refiere el artículo 37.1, cuando sea posible.

2. Cada encargado del tratamiento llevará un registro de todas las actividades de tratamiento de datos personales efectuadas en nombre de un responsable. Este registro contendrá la información siguiente:

a) El nombre y los datos de contacto del encargado o encargados del tratamiento, de cada responsable del tratamiento en cuyo nombre actúe el encargado y, en su caso, del delegado de protección de datos.
b) Las categorías de tratamientos efectuados en nombre de cada responsable.
c) Las transferencias de datos personales a un Estado que no sea miembro de la Unión Europea o a una organización internacional, en su caso, incluida la identificación de dicho Estado o de dicha organización internacional cuando el responsable del tratamiento así lo ordene explícitamente.
d) La descripción general de las medidas técnicas y organizativas de seguridad a las que se refiere el artículo 37.1, cuando sea posible.

3. Los registros referidos en este artículo se establecerán y llevarán por escrito, incluida la posibilidad del formato electrónico.
Estos registros estarán a disposición de la autoridad de protección de datos competente, a solicitud de esta, de conformidad con lo dispuesto legalmente.
4. Los responsables de los tratamientos harán público el registro de sus actividades de tratamiento, accesible por medios electrónicos, en el que constará la información a la que se refiere el apartado 1.

Artículo 33. *Registro de operaciones.*

1. Los responsables y encargados del tratamiento deberán mantener registros de, al menos, las siguientes operaciones de tratamiento en sistemas de tratamiento automatizados: recogida, alteración, consulta, comunicación, incluidas las transferencias, y combinación o supresión. Los registros de consulta y comunicación harán posible determinar la justificación, la fecha y la hora de tales operaciones y, en la medida de lo posible, el nombre de la persona que consultó o comunicó los datos personales, así como la identidad de los destinatarios de dichos datos personales.

2. Estos registros se utilizarán únicamente a efectos de verificar la legalidad del tratamiento, controlar el cumplimiento de las medidas y de las políticas de protección de datos y garantizar la integridad y la seguridad de los datos personales en el ámbito de los procesos penales.

Dichos registros estarán a disposición de la autoridad de protección de datos competente a solicitud de esta, de conformidad con lo dispuesto legalmente.

Artículo 34. *Cooperación con las autoridades de protección de datos.*

El responsable y el encargado del tratamiento cooperarán con la autoridad de protección de datos competente, en el marco de la legislación vigente, cuando esta lo solicite en el desempeño de sus funciones.

Artículo 35. *Evaluación de impacto relativa a la protección de datos.*

1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, suponga por su naturaleza, alcance, contexto o fines, un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, con carácter previo, una evaluación del impacto de las operaciones de tratamiento previstas en la protección de datos personales.

2. La evaluación incluirá, como mínimo, una descripción general de las operaciones de tratamiento previstas, una evaluación de riesgos para los derechos y libertades de los interesados, las medidas contempladas para hacer frente a estos peligros, así como las medidas de seguridad y mecanismos destinados a garantizar la protección de los datos personales y a demostrar su conformidad con esta Ley Orgánica. Esta evaluación tendrá en cuenta los derechos e intereses legítimos de los interesados y de las demás personas afectadas.

3. Las autoridades de protección de datos podrán establecer una lista de tratamientos que estén sujetos a la realización de una evaluación de impacto con arreglo a lo dispuesto en el apartado anterior y, del mismo modo, podrán establecer una lista de tratamientos que no estén sujetos a esta obligación. Ambas listas tendrán un carácter meramente orientativo.

Artículo 36. *Consulta previa a la autoridad de protección de datos.*

1. El responsable o el encargado del tratamiento consultará a la autoridad de protección de datos, antes de proceder al tratamiento de datos personales que vayan a formar parte de un nuevo fichero, en cualquiera de las siguientes circunstancias:

a) Cuando la evaluación del impacto en la protección de los datos indique que el tratamiento entrañaría un alto nivel de riesgo, a falta de medidas adoptadas por el responsable para mitigar el riesgo o los posibles daños.

b) Cuando el tipo de tratamiento pueda generar un alto nivel de riesgo para los derechos y libertades de los interesados, en particular, cuando se usen tecnologías, mecanismos o procedimientos nuevos.

2. La autoridad de protección de datos correspondiente podrá establecer una lista de carácter orientativo, de las operaciones de tratamiento sujetas a consulta previa, con arreglo a lo dispuesto en el apartado anterior.

3. El responsable del tratamiento facilitará a la autoridad de protección de datos competente, la evaluación de impacto contemplada en el artículo 35 y, previa solicitud, cualquier información adicional que permita a dicha autoridad de protección de datos evaluar la conformidad del tratamiento y, más concretamente, el nivel de riesgo para la protección de los datos personales del interesado y las garantías correspondientes.

4. Cuando la autoridad de protección de datos considere que el tratamiento previsto en el apartado 1 pudiera infringir lo dispuesto en esta Ley Orgánica deberá, en un plazo de seis semanas desde la solicitud de la consulta, asesorar por escrito al responsable del tratamiento y, en su caso, al encargado del tratamiento, en especial, cuando el responsable del tratamiento no haya identificado o mitigado suficientemente el peligro o el nivel de riesgo. Asimismo, la autoridad de protección de datos podrá ejercer cualquiera de sus potestades de investigación, corrección o consulta.

Este plazo podrá prorrogarse un mes, en función de la complejidad del tratamiento previsto. La autoridad de protección de datos informará al responsable y, en su caso, al encargado acerca de la prórroga, en el plazo de un mes a partir de la recepción de la solicitud de consulta, junto con los motivos de la dilación.

En caso de no contestar a la consulta en el plazo previsto, no operará la presunción del carácter favorable del mismo.

Sección 2.ª Seguridad de los datos personales

Artículo 37. *Seguridad del tratamiento.*

1. El responsable y el encargado del tratamiento, teniendo en cuenta el estado de la técnica y los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los niveles de riesgo para los derechos y libertades de las personas físicas, aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado, especialmente en lo relativo al tratamiento de las categorías de datos personales a las que se refiere el artículo 13. En particular, deberán aplicar a los tratamientos de datos personales las medidas incluidas en el Esquema Nacional de Seguridad.

2. Por lo que respecta al tratamiento automatizado, el responsable o encargado del tratamiento, a raíz de una evaluación de los riesgos, pondrá en práctica medidas de control con el siguiente propósito:

a) En el control de acceso a los equipamientos, denegar el acceso a personas no autorizadas a los equipamientos utilizados para el tratamiento.

b) En el control de los soportes de datos, impedir que estos puedan ser leídos, copiados, modificados o cancelados por personas no autorizadas.

c) En el control del almacenamiento, impedir que se introduzcan sin autorización datos personales, o que estos puedan inspeccionarse, modificarse o suprimirse sin autorización.

d) En el control de los usuarios, impedir que los sistemas de tratamiento automatizado puedan ser utilizados por personas no autorizadas por medio de instalaciones de transmisión de datos.

e) En el control del acceso a los datos, garantizar que las personas autorizadas a utilizar un sistema de tratamiento automatizado, sólo puedan tener acceso a los datos personales para los que han sido autorizados.

f) En el control de la transmisión, garantizar que sea posible verificar y establecer a qué organismos se han transmitido o pueden transmitirse, o a cuya disposición pueden ponerse los datos personales mediante equipamientos de comunicación de datos.

g) En el control de la introducción, garantizar que pueda verificarse y constatarse, a posteriori, qué datos personales se han introducido en los sistemas de tratamiento automatizado, en qué momento y quién los ha introducido.

h) En el control del transporte, impedir que durante las transferencias de datos personales o durante el transporte de soportes de datos, los datos personales puedan ser leídos, copiados, modificados o suprimidos sin autorización.

i) En el control de restablecimiento, garantizar que los sistemas instalados puedan restablecerse en caso de interrupción.

j) En el control de fiabilidad e integridad, garantizar que las funciones del sistema no presenten defectos, que los errores de funcionamiento sean señalados y que los datos personales almacenados no se degraden por fallos de funcionamiento del sistema.

Artículo 38. *Notificación a la autoridad de protección de datos de una violación de la seguridad de los datos personales.*

1. Cualquier violación de la seguridad de los datos personales será notificada por el responsable del tratamiento a la autoridad de protección de datos competente, a menos que sea improbable que la violación de la seguridad de los datos personales constituya un peligro para los derechos y las libertades de las personas físicas.

La notificación deberá realizarse en el plazo de las setenta y dos horas siguientes al momento en que se haya tenido constancia de ella. En caso contrario, deberá ir acompañada de los motivos de la dilación.

2. El encargado del tratamiento notificará, sin dilación indebida, al responsable del tratamiento, las violaciones de la seguridad de los datos personales de las que tenga conocimiento.

3. La notificación contemplada en el apartado 1 deberá, al menos:

a) Referir la naturaleza de la violación de la seguridad de los datos personales, incluyendo, cuando sea posible, las categorías y el número aproximado de personas afectadas, así como las categorías y el número aproximado de registros de datos personales afectados por la violación de la seguridad.

b) Comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.

c) Detallar las posibles consecuencias de la violación de la seguridad de los datos personales.

d) Describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar sus posibles efectos negativos.

4. Si no fuera posible facilitar la información simultáneamente, se podrá facilitar de forma progresiva, a medida que se disponga de ella.

5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relativos a dicha violación, sus efectos y las medidas correctivas adoptadas.

Dicha documentación estará a disposición de la autoridad de protección de datos competente al objeto de verificar el cumplimiento de lo dispuesto en este artículo.

6. Cuando la violación de la seguridad de los datos personales afecte a datos que hayan sido transmitidos por el responsable del tratamiento o al responsable del tratamiento de otro Estado miembro de la Unión Europea, la información recogida en el apartado 3 se comunicará al responsable del tratamiento de dicho Estado.

7. Todas las actividades relacionadas en este artículo se realizarán sin dilaciones indebidas.

Artículo 39. *Comunicación de una violación de la seguridad de los datos personales al interesado.*

1. Cuando existan indicios de que una violación de la seguridad de los datos personales supondría un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento comunicará al interesado, sin dilación indebida, la violación de la seguridad de los datos personales.

2. La comunicación al interesado describirá con lenguaje claro, sencillo y accesible conforme a sus circunstancias y capacidades, la naturaleza de la violación de la seguridad de los datos personales y contendrá, al menos, la información y las medidas a las que se refiere el artículo 38.3. b), c) y d).

3. No se efectuará la comunicación al interesado que prevé el apartado 1 cuando se cumpla alguna de las condiciones siguientes:

a) Que el responsable del tratamiento haya adoptado medidas apropiadas de protección técnica y organizativa y dichas medidas se hayan aplicado a los datos personales afectados por la violación de la seguridad antes de la misma, en particular, aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como en el caso del cifrado.

b) Que el responsable del tratamiento haya tomado medidas ulteriores para garantizar que no se materialice el alto nivel de riesgo para los derechos y libertades del interesado a que hace referencia el apartado 1.

c) Que suponga un esfuerzo desproporcionado, en cuyo caso, se optará por su publicación en el boletín oficial correspondiente, en la sede electrónica del responsable del tratamiento o en otro canal oficial que permita una comunicación efectiva con el interesado.

4. En el supuesto de que el responsable del tratamiento no haya comunicado al interesado la violación de la seguridad de los datos personales, la autoridad de protección de datos competente, una vez valorada la existencia de un alto nivel de riesgo, podrá exigirle que proceda a dicha comunicación, o bien que determine la concurrencia de alguna de las condiciones previstas en el apartado 3.

5. La comunicación al interesado referida en el apartado 1 podrá aplazarse, limitarse u omitirse con sujeción a las condiciones y por los motivos previstos en el artículo 24.

Sección 3.ª Delegado de protección de datos

Artículo 40. *Designación del delegado de protección de datos.*

1. Los responsables del tratamiento designarán, en todo caso, un delegado de protección de datos. No estarán obligados a designarlo los órganos jurisdiccionales o el Ministerio Fiscal cuando el tratamiento de datos personales se realice en el ejercicio de sus funciones jurisdiccionales.

2. El delegado de protección de datos será designado atendiendo a sus cualidades profesionales. En concreto, se tendrán en cuenta sus conocimientos especializados en legislación, su experiencia en materia de protección de datos y su capacidad para desempeñar las funciones a las que se refiere el artículo 42. En el caso de haber designado un delegado de protección de datos al amparo del Reglamento General de Protección de Datos, este será el que asumirá las funciones de delegado de protección de datos previstas en esta Ley Orgánica.

3. Podrá designarse a un único delegado de protección de datos para varias autoridades competentes, teniendo en cuenta la estructura organizativa y el tamaño de estas.

4. Los responsables del tratamiento publicarán los datos de contacto del delegado de protección de datos y comunicarán a la autoridad de protección de datos competente su designación y cese, en el plazo de diez días desde que se haya producido.

Artículo 41. *Posición del delegado de protección de datos.*

1. El responsable del tratamiento velará porque el delegado de protección de datos participe adecuada y oportunamente en todas las cuestiones relativas a la protección de datos personales, al tiempo que cuidará de que mantenga sus conocimientos especializados, cuente con los recursos necesarios para el desempeño de sus funciones y acceda a los datos personales y a las operaciones de tratamiento.

2. El delegado de protección de datos no podrá ser removido ni sancionado por el responsable o el encargado por desempeñar sus funciones, salvo que incurriera en dolo o negligencia grave en su ejercicio. Se garantizará la independencia del delegado de protección de datos dentro de la organización, debiendo evitar cualquier conflicto de intereses.

3. En el ejercicio de sus funciones el delegado de protección de datos tendrá acceso a los datos personales y procesos de tratamiento. La existencia de cualquier deber de confidencialidad o secreto no permitirá que el responsable o el encargado del tratamiento se oponga a dicho acceso.

4. Cuando el delegado de protección de datos aprecie la existencia de una vulneración relevante en materia de protección de datos lo documentará y lo comunicará inmediatamente a los órganos de dirección del responsable o del encargado del tratamiento.

Artículo 42. *Funciones del delegado de protección de datos.*

El responsable del tratamiento encomendará al delegado de protección de datos, al menos, las siguientes funciones:

a) Informar y asesorar al responsable del tratamiento y a los empleados que se ocupen del mismo, acerca de las obligaciones que les incumben en virtud de esta Ley Orgánica y de otras disposiciones de protección de datos aplicables.

b) Supervisar el cumplimiento de lo dispuesto en esta Ley Orgánica y en otras disposiciones de protección de datos aplicables, así como de lo establecido en las políticas del responsable del tratamiento en materia de protección de datos personales, incluidas la

asignación de responsabilidades, la concienciación y formación del personal que participe en las operaciones de tratamiento y las auditorías correspondientes.

c) Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su realización.

d) Cooperar con la autoridad de protección de datos en los términos de la legislación vigente.

e) Actuar como punto de contacto de la autoridad de protección de datos para las cuestiones relacionadas con el tratamiento, incluida la consulta previa referida en el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.

CAPÍTULO V

Transferencias de datos personales a terceros países que no sean miembros de la Unión Europea o a organizaciones internacionales

Artículo 43. *Principios generales de las transferencias de datos personales.*

1. Al objeto de garantizar el nivel de protección de las personas físicas previsto en esta Ley Orgánica, cualquier transferencia de datos personales realizada por las autoridades competentes españolas a un Estado que no sea miembro de la Unión Europea o a una organización internacional, incluidas las transferencias ulteriores a otro Estado que no pertenezca a la Unión Europea o a otra organización internacional, deberá cumplir las siguientes condiciones:

a) Que la transferencia sea necesaria para los fines establecidos en el artículo 1.

b) Que los datos personales sean transferidos a un responsable del tratamiento competente para los fines mencionados en el artículo 1.

c) Que, en caso de que los datos personales hayan sido transferidos a la autoridad competente española procedentes de otro Estado miembro de la Unión Europea, dicho Estado miembro autorice previamente la transferencia ulterior de conformidad con su Derecho nacional.

d) Que la Comisión Europea haya adoptado una decisión de adecuación de acuerdo con el artículo 44 o, a falta de dicha decisión, cuando se hayan aportado o existan garantías apropiadas de conformidad con el artículo 45 o, a falta de ambas, cuando resulten de aplicación las excepciones para situaciones específicas de acuerdo con el artículo 46.

e) Cuando se trate de una transferencia ulterior a un Estado que no sea miembro de la Unión Europea u organización internacional, de datos transferidos inicialmente por una autoridad competente española, esta autorizará la transferencia ulterior, una vez considerados todos los factores pertinentes, entre estos, la gravedad de la infracción penal, la finalidad para la que se transfirieron inicialmente los datos personales y el nivel de protección existente en ese Estado u organización internacional a los que se transfieran ulteriormente los datos personales.

2. Las transferencias de datos personales por las autoridades españolas sin autorización previa de otro Estado miembro, conforme al párrafo 1c), sólo se permitirán si la transferencia de datos personales resulta necesaria para prevenir una amenaza inmediata y grave para la seguridad pública, tanto de un Estado miembro de la Unión Europea como no perteneciente a la misma, o para los intereses fundamentales de un Estado miembro de la Unión Europea, y cuando la autorización previa no pueda conseguirse a su debido tiempo.

Las autoridades españolas informarán sin dilación a la autoridad responsable de conceder la autorización previa, y en todo caso en el plazo máximo de diez días a contar desde que se haya producido la transferencia.

3. Se impulsará el establecimiento de mecanismos de cooperación internacional y de asistencia mutua y se fomentará el intercambio de normativa y de buenas prácticas con los Estados que no sean miembros de la Unión Europea y con las organizaciones internacionales, de manera que se facilite la aplicación efectiva de la legislación sobre la protección de datos personales, inclusive en el ámbito de la resolución de conflictos jurisdiccionales, procurando la participación de todas las partes interesadas.

Artículo 44. *Transferencias basadas en una decisión de adecuación.*

1. Cuando la Comisión Europea, mediante una decisión de adecuación, haya decidido que un Estado que no sea miembro de la Unión Europea, un territorio o uno o varios sectores específicos de dicho Estado, o la organización internacional de que se trate, garantizan un nivel de protección adecuado, podrán realizarse transferencias de datos personales a ese Estado u organización internacional. Dichas transferencias no requerirán ninguna autorización específica.

2. Toda decisión de adecuación de la Comisión Europea que determine que un Estado que no sea miembro de la Unión Europea, un territorio o uno o varios sectores específicos de dicho Estado, o una organización internacional ha dejado de garantizar un nivel de protección adecuado, se entenderá sin perjuicio de las transferencias de datos personales a dicho Estado, territorio o sector del mismo o a la organización internacional de que se trate, en virtud de los artículos 45 y 46.

Artículo 45. *Transferencias mediante garantías apropiadas.*

1. En ausencia de una decisión de adecuación de la Comisión Europea conforme al artículo 44 podrán realizarse transferencias de datos personales a un Estado que no sea miembro de la Unión Europea o a una organización internacional cuando concurra alguna de las siguientes circunstancias:

a) Se hayan aportado garantías apropiadas respecto a la protección de datos personales en un instrumento jurídicamente vinculante.

b) Se hayan evaluado, por parte del responsable del tratamiento, todas las circunstancias que concurren en la transferencia de datos personales y se haya concluido que existen garantías apropiadas respecto a la protección de datos personales.

2. El responsable del tratamiento informará a la autoridad de protección de datos competente acerca de las categorías de transferencias a tenor del párrafo 1.b).

3. Cuando las transferencias se basen en lo dispuesto en el párrafo 1.b) deberán documentarse. La documentación se pondrá a disposición de la autoridad de protección de datos competente, previa solicitud, con inclusión de la siguiente información: fecha, hora de la transferencia, información sobre la autoridad competente destinataria, justificación de la transferencia y datos personales transferidos.

Artículo 46. *Excepciones para situaciones específicas.*

1. En ausencia de una decisión de adecuación de la Comisión Europea o de garantías apropiadas de acuerdo con los artículos 44 y 45, podrán realizarse transferencias de datos personales a un Estado que no sea miembro de la Unión Europea o a una organización internacional cuando la transferencia sea necesaria por concurrir alguna de las siguientes circunstancias:

a) Para proteger los intereses vitales o los derechos y libertades fundamentales del interesado o de otra persona.

b) Para salvaguardar intereses legítimos del interesado reconocidos por la legislación española.

c) Para prevenir una amenaza grave e inmediata para la seguridad pública de un Estado, tanto miembro de la Unión Europea como no perteneciente a la misma.

d) En casos individuales, a efectos del artículo 1.

e) Para el ejercicio, en un caso individual, de acciones legales o para la defensa frente a ellas en relación con los fines incluidos en el artículo 1.

2. Los datos personales no se transferirán, si la autoridad competente de la transferencia determina que los derechos y libertades fundamentales del interesado prevalecen sobre el interés público en la transferencia, establecido en las letras d) y e) del apartado anterior.

3. Las transferencias basadas en lo dispuesto en este artículo deberán documentarse. Esta documentación quedará a disposición de la autoridad de protección de datos competente, con inclusión de la fecha y la hora de la transferencia, la información sobre la

autoridad competente destinataria, la justificación de la transferencia y los datos personales transferidos.

Artículo 47. *Transferencias directas de datos personales a destinatarios, que no sean autoridades competentes, establecidos en Estados no pertenecientes a la Unión Europea.*

1. Excepcionalmente, en casos particulares y específicos y sin perjuicio de la existencia de un acuerdo internacional entre España y un Estado que no sea miembro de la Unión Europea en el ámbito de la cooperación judicial penal o de la cooperación policial, las autoridades competentes españolas podrán transferir datos personales directamente a destinatarios que no tengan la condición de autoridad competente, establecidos en Estados que no sean miembros de la Unión Europea, siempre que se cumplan las disposiciones de esta Ley Orgánica y se satisfagan todas las condiciones siguientes:

a) Que la transferencia sea estrictamente necesaria para la realización de una función de la autoridad competente que lleva a cabo la transferencia conforme al Derecho de la Unión Europea o a la legislación española, con cualquiera de los fines del artículo 1.

b) Que la autoridad competente que realiza la transferencia determine que ninguno de los derechos y libertades fundamentales del interesado son superiores al interés público que precise de la transferencia de que se trate.

c) Que la autoridad competente que realiza la transferencia considere que la transferencia a una autoridad competente del Estado en el que está establecido el destinatario, con cualquiera de los fines del artículo 1, resultaría ineficaz o inadecuada, en particular porque la transferencia no pueda efectuarse dentro de plazo.

d) Que se informe sin dilación indebida a la autoridad competente para los fines que contempla el artículo 1 de dicho Estado, salvo que esto resulte ineficaz o inadecuado.

e) Que la autoridad competente que realiza la transferencia informe al destinatario de la finalidad o finalidades específicas para las que puede tratar los datos personales, siempre y cuando dicho tratamiento sea necesario.

2. La autoridad competente que realiza la transferencia informará a la autoridad de protección de datos competente acerca de las transferencias efectuadas a tenor de este artículo.

3. Las transferencias basadas en lo dispuesto en este artículo deberán documentarse.

CAPÍTULO VI

Autoridades de Protección de Datos Independientes

Artículo 48. *Autoridades de protección de datos.*

A los efectos de esta Ley Orgánica son autoridades de protección de datos independientes:

a) La Agencia Española de Protección de Datos.

b) Las autoridades autonómicas de protección de datos, exclusivamente en relación a aquellos tratamientos de los que sean responsables en su ámbito de competencia, y conforme a lo dispuesto en el artículo 57.1 de la Ley Orgánica 3/2018, de 5 de diciembre, y en la normativa autonómica aplicable.

Dichas autoridades se regirán por esta Ley Orgánica respecto de los tratamientos sometidos a la misma, de acuerdo con los principios de cooperación institucional, coordinación de criterios e información mutua, y por lo establecido en el Título VII de la Ley Orgánica 3/2018, de 5 de diciembre, y en sus normas de creación, así como por lo que establezcan sus normas de desarrollo.

La Agencia Española de Protección de Datos actuará como representante de las autoridades de protección de datos en el Comité Europeo de Protección de Datos.

Artículo 49. *Funciones.*

1. Las autoridades de protección de datos ejercerán, respecto de los tratamientos sometidos a esta Ley Orgánica, las siguientes funciones:

a) Supervisar y hacer cumplir las disposiciones adoptadas con arreglo a esta Ley Orgánica.

b) Promover la sensibilización y la comprensión de la ciudadanía acerca de los riesgos, normas, garantías y derechos relativos al tratamiento.

c) Asesorar a las Cortes Generales, al Gobierno de la Nación y a los organismos dependientes o vinculados a la Administración General del Estado, así como, de acuerdo con su ámbito competencial, a las Asambleas Legislativas de las comunidades autónomas, los Consejos de Gobierno y los organismos dependientes o vinculados a la Administración de las comunidades autónomas, acerca de las medidas legislativas y administrativas relativas a la protección de los derechos y libertades de las personas físicas con respecto al tratamiento.

d) Promover la sensibilización de los responsables y encargados del tratamiento en relación con las obligaciones que les incumben.

e) Facilitar la información solicitada por los interesados sobre el ejercicio de sus derechos en virtud de esta Ley Orgánica y, en su caso, cooperar a tal fin con las autoridades de protección de datos de otros Estados miembros de la Unión Europea.

f) Tramitar y responder las reclamaciones presentadas por un interesado o por una entidad, organización o asociación de conformidad con el artículo 55, e investigar, en la medida oportuna, el motivo de la reclamación e informar al reclamante sobre el curso y el resultado de la investigación en un plazo razonable.

g) Controlar, de acuerdo con lo dispuesto en el artículo 25, la licitud del tratamiento e informar al interesado en un plazo razonable sobre el resultado del control o sobre los motivos por los que no se ha llevado a cabo.

h) Cooperar, en particular compartiendo información, con otras autoridades de protección de datos y prestarse asistencia mutua.

i) Llevar a cabo investigaciones sobre la aplicación de esta Ley Orgánica, en particular basándose en la información recibida de otra autoridad de protección de datos u otra autoridad pública.

j) Realizar un seguimiento de acontecimientos que sean de interés, en la medida en que tengan incidencia en la protección de datos personales, de manera concreta sobre el desarrollo de las tecnologías de la información y la comunicación.

k) Prestar asesoramiento sobre las operaciones de tratamiento contempladas en el artículo 36.

l) Contribuir a las actividades del Comité Europeo de Protección de Datos.

m) Informar todas las disposiciones legales o reglamentarias que afecten a tratamientos sometidos a esta Ley Orgánica.

2. Las autoridades de protección de datos adoptarán medidas tendentes a facilitar la formulación de las reclamaciones incluidas en el párrafo 1f), tales como proporcionar formularios que puedan cumplimentarse electrónicamente, sin excluir otros medios.

3. El desempeño de las funciones de las autoridades de control no implicará coste alguno para el interesado ni para el delegado de protección de datos.

4. Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, la autoridad de protección de datos podrá negarse a actuar respecto de la solicitud. La carga de la demostración del carácter manifiestamente infundado o excesivo de la solicitud recaerá en la autoridad de protección de datos.

Artículo 50. *Potestades.*

Las autoridades de protección de datos tendrán atribuidas, en el ámbito de esta Ley Orgánica, las siguientes potestades:

a) De investigación, incluyendo el acceso a todos los datos que estén siendo tratados por el responsable o el encargado del tratamiento, en los términos previstos por la legislación vigente.

b) De advertencia y control de lo exigido en esta Ley Orgánica, incluida la sanción de las infracciones cometidas, la elaboración de recomendaciones, órdenes de rectificación, supresión o limitación del tratamiento de datos personales o de limitación temporal o definitiva del tratamiento, incluida su prohibición, así como la orden a los responsables del tratamiento de comunicar las vulneraciones de seguridad de los datos a los interesados.

c) De asesoramiento, que comprende la consulta previa prevista en el artículo 36 y la emisión, por propia iniciativa o previa solicitud, de dictámenes destinados a las Cortes Generales o al Gobierno, a otras instituciones u organismos, así como al público en general, acerca de todo asunto relacionado con la protección de datos personales sujeto a esta Ley Orgánica.

Artículo 51. *Asistencia entre autoridades de protección de datos de los Estados miembros de la Unión Europea.*

1. Las autoridades de protección de datos españolas facilitarán la asistencia y cooperación necesaria a las autoridades de protección de datos de otros Estados miembros de la Unión Europea, debiendo responder a las solicitudes de estas sin dilación indebida, y en cualquier caso, en el plazo máximo de un mes desde su recepción. La asistencia mutua abarcará, en particular, las solicitudes de información y las medidas de control, así como las solicitudes para llevar a cabo consultas, inspecciones e investigaciones.

2. Las autoridades de protección de datos españolas podrán solicitar, en el ejercicio de sus funciones, la asistencia y cooperación de las autoridades de protección de datos de otros Estados miembros de la Unión Europea.

Las solicitudes deberán contener toda la información necesaria para su contestación, incluidos los motivos y la finalidad de la solicitud. La información intercambiada se utilizará únicamente para el fin para el que haya sido solicitada.

3. Las contestaciones de las autoridades de protección de datos españolas deberán indicar los resultados obtenidos o las medidas adoptadas con base en la solicitud recibida. Estas respuestas serán remitidas en formato electrónico, en la medida de lo posible.

4. La solicitud de asistencia procedente de una autoridad de protección de datos de un Estado miembro de la Unión Europea únicamente podrá negarse a ser atendida, de manera motivada, cuando la autoridad de protección de datos española no sea competente respecto al objeto o a las medidas solicitadas, o bien cuando el hecho de atender la solicitud vulnere la legislación española o el Derecho de la Unión Europea. Se informará, en su caso, de la restricción de los derechos del interesado adoptada en aplicación del artículo 24.

5. Las medidas adoptadas con ocasión de una solicitud de asistencia mutua serán gratuitas, sin perjuicio de que en circunstancias excepcionales puedan pactarse indemnizaciones por gastos específicos derivados de la prestación de la asistencia.

CAPÍTULO VII

Reclamaciones

Artículo 52. *Régimen aplicable a los procedimientos tramitados ante las autoridades de protección de datos.*

1. En el caso de que los interesados aprecien que el tratamiento de los datos personales haya infringido las disposiciones de esta Ley Orgánica o no haya sido atendida su solicitud de ejercicio de los derechos reconocidos en los artículos 21, 22 y 23 tendrán derecho a presentar una reclamación ante la autoridad de protección de datos.

2. Dichas reclamaciones serán tramitadas por la autoridad de protección de datos competente con sujeción al procedimiento establecido en el título VIII de la Ley Orgánica 3/2018, de 5 de diciembre, y, en su caso, a la legislación de las Comunidades Autónomas que resulte de aplicación. Tendrán carácter subsidiario las normas generales sobre los procedimientos administrativos y el régimen jurídico del sector público.

3. En el caso de que la actuación provenga de un órgano judicial o del Ministerio Fiscal cuando se realice el tratamiento con fines jurisdiccionales la responsabilidad se regirá por lo dispuesto en el Título V del Libro III de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

4. Sin perjuicio de lo dispuesto en el artículo 55, todo interesado tendrá derecho a interponer recurso contencioso-administrativo, de acuerdo con su normativa reguladora, en caso de que la autoridad de protección de datos competente no dicte resolución expresa y se la notifique en el plazo de tres meses.

Artículo 53. *Derecho a indemnización por entes del sector público.*

1. Los interesados tendrán derecho a ser indemnizados por el responsable del tratamiento, o por el encargado del tratamiento cuando formen parte del sector público, en el caso de que sufran daño o lesión en sus bienes o derechos como consecuencia del incumplimiento de lo dispuesto en esta Ley Orgánica.

2. Cuando quien incumpla lo dispuesto en esta Ley Orgánica tenga la consideración de Administración pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad patrimonial previsto en la normativa sobre el procedimiento administrativo común de las Administraciones públicas y sobre el régimen jurídico del sector público.

3. En el caso de que la actuación provenga de un órgano judicial o del Ministerio Fiscal cuando se realice el tratamiento con fines jurisdiccionales la responsabilidad se regirá por lo dispuesto en el Título V del Libro III de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

Artículo 54. *Derecho a indemnización por encargados del tratamiento del sector privado.*

1. Los interesados que sufran daño o lesión en sus bienes o derechos por parte del encargado del tratamiento que no forme parte del sector público, como consecuencia del incumplimiento de lo dispuesto en esta Ley Orgánica, tendrán derecho a ser indemnizados.

2. El encargado del tratamiento estará obligado a indemnizar todos los daños y perjuicios que cause a los interesados o a terceros como resultado de las operaciones de tratamientos de datos previstas en el contrato u otro instrumento o acto jurídico suscrito con el responsable del tratamiento conforme al artículo 30, de conformidad con el régimen de responsabilidad del contratista por los daños causados a terceros regulado en la normativa sobre contratos del sector público.

3. Cuando tales daños y perjuicios hayan sido ocasionados como consecuencia inmediata y directa de una orden de la autoridad competente responsable del tratamiento, será esta la responsable.

4. Los interesados o los terceros perjudicados podrán requerir al responsable del tratamiento, dentro del año siguiente a la producción del hecho, para que informe, una vez oído el encargado del tratamiento, acerca de a cuál de las partes contratantes o de las que hayan suscrito el acto jurídico conforme al artículo 30, corresponde la responsabilidad de los daños. El ejercicio de esta facultad interrumpe el plazo de prescripción de la acción.

5. Con independencia de lo previsto en los apartados anteriores, el encargado del tratamiento que no forme parte del sector público responderá de los daños y perjuicios que durante las operaciones de tratamiento de datos cause. Deberá hacerlo tanto respecto del responsable del tratamiento, como respecto del interesado o de terceros por incumplimientos de esta Ley Orgánica, de infracciones de preceptos legales o reglamentarios, o por el incumplimiento de las previsiones contenidas en el contrato o en otro acto jurídico suscrito. El encargado del tratamiento que no forme parte del sector público deberá haber incurrido en actuaciones que le sean imputables, sin perjuicio de la aplicación del régimen sancionador, en su caso.

Artículo 55. *Tutela judicial efectiva.*

1. Sin perjuicio de cualquier otro recurso administrativo o reclamación, toda persona física o jurídica tendrá derecho a recurrir ante la jurisdicción contencioso-administrativa, de acuerdo con su legislación reguladora, contra los actos y resoluciones dictadas por la autoridad de protección de datos competente.

2. El interesado podrá conferir su representación a una entidad, organización o asociación sin ánimo de lucro que haya sido correctamente constituida, cuyos objetivos estatutarios sean de interés público y que actúe en el ámbito de la protección de los

derechos y libertades de los interesados en materia de protección de sus datos personales, para que ejerza los derechos contemplados en el apartado anterior.

CAPÍTULO VIII

Régimen sancionador

Artículo 56. *Sujetos responsables.*

1. La responsabilidad por las infracciones cometidas recaerá directamente en los sujetos obligados que, por acción u omisión, realizaran la conducta en que consista la infracción.
2. Están sujetos al régimen sancionador:

a) Los responsables de los tratamientos.
b) Los encargados de los tratamientos.
c) Los representantes de los encargados no establecidos en el territorio de la Unión Europea.
d) El resto de las personas físicas o jurídicas obligadas por el contenido del deber de colaboración establecido en el artículo 7.

3. No será de aplicación el régimen sancionador establecido en este capítulo al delegado de protección de datos.

Artículo 57. *Concurso de normas.*

1. Los hechos susceptibles de ser calificados con arreglo a dos o más preceptos de esta u otra Ley, siempre que no constituyan infracciones al Reglamento General de Protección de Datos, ni a la Ley Orgánica 3/2018, de 5 de diciembre, se sancionarán observando las siguientes reglas:

a) El precepto especial se aplicará con preferencia al general.
b) El precepto más amplio o complejo absorberá el que sancione las infracciones subsumidas en aquel.
c) En defecto de los criterios anteriores, se aplicará el precepto que sancione los hechos con la sanción mayor.

2. En el caso de que un solo hecho constituya dos o más infracciones, o cuando una de ellas sea medio necesario para cometer la otra, la conducta será sancionada por aquella infracción que conlleve una mayor sanción.

Artículo 58. *Infracciones muy graves.*

Son infracciones muy graves:

a) El tratamiento de datos personales que vulnere los principios y garantías establecidos en el artículo 6 o sin que concurra alguna de las condiciones de licitud del tratamiento establecidas en el artículo 11, siempre que se causen perjuicios de carácter muy grave a los interesados.
b) El acceso, cesión, alteración y divulgación de los datos al margen de los supuestos autorizados por el responsable o encargado de los datos, siempre que no constituya ilícito penal.
c) La transferencia temporal o definitiva de datos de carácter personal con destino a Estados que no sean miembros de la Unión Europea o a destinatarios que no sean autoridades competentes, establecidos en dichos Estados incumpliendo las condiciones previstas en los artículos 43 y 47.
d) La utilización de los datos para una finalidad que no sea compatible con el objetivo para el que fueron recogidos o cuando no se cumplan las condiciones establecidas en el artículo 6, siempre que no se cuente con una base legal para ello.
e) El tratamiento de datos personales de las categorías especiales sin que concurra alguna de las circunstancias previstas en el artículo 13 o sin garantizar las medidas de seguridad adecuadas, que cause perjuicios graves a los interesados.

f) La omisión del deber de informar al interesado acerca del tratamiento de sus datos de carácter personal conforme a lo dispuesto en esta Ley Orgánica.

g) La vulneración del deber de confidencialidad del encargado del tratamiento, establecido en el artículo 30.

h) La adopción de decisiones individuales automatizadas sin las garantías señaladas en el artículo 14, siempre que se causen perjuicios de carácter muy grave para los interesados.

i) El impedimento, la obstaculización o la falta de atención reiterada del ejercicio de los derechos del interesado de acceso, rectificación, supresión de sus datos o limitación del tratamiento, siempre que se causen perjuicios de carácter muy grave para los interesados.

j) La negativa a proporcionar a las autoridades competentes la información necesaria para la prevención, detección, investigación y enjuiciamiento de infracciones penales, para la ejecución de sanciones penales o para la protección y prevención frente a las amenazas contra la seguridad pública de acuerdo con lo previsto en el artículo 7, así como a informar al interesado cuando se comuniquen sus datos en virtud del deber de colaboración establecido en dicho artículo.

k) La resistencia u obstrucción del ejercicio de la función inspectora de las autoridades de protección de datos competentes.

l) La falta de notificación a las autoridades de protección de datos competentes acerca de una violación de la seguridad de los datos personales, cuando sea exigible, así como la ausencia de comunicación al interesado de una violación de la seguridad cuando sea procedente de acuerdo con el artículo 39, siempre que se deriven perjuicios de carácter muy grave para el interesado.

m) El incumplimiento de las resoluciones dictadas por las autoridades de protección de datos competentes, en el ejercicio de las potestades que le confiere el artículo 50.

n) No facilitar el acceso del personal de las autoridades de protección de datos competentes a los datos personales, información, locales, equipos y medios de tratamiento, cuando sean requeridos por las mismas, en el ejercicio de sus poderes de investigación.

ñ) El incumplimiento de los plazos de conservación y revisión establecidos en virtud del artículo 8.

Artículo 59. *Infracciones graves.*

Son infracciones graves:

a) El tratamiento de los datos de carácter personal cuando se incumplan los principios del artículo 6 o las condiciones de licitud del tratamiento del artículo 11, siempre que no constituya una infracción muy grave.

b) El tratamiento de datos personales de las categorías especiales sin que concurra alguna de las circunstancias previstas en el artículo 13 o sin garantizar las medidas de seguridad adecuadas, siempre que no constituya una infracción muy grave.

c) La adopción de decisiones individuales automatizadas sin las garantías señaladas en el artículo 14, siempre que no constituya una infracción muy grave.

d) La falta de designación de un delegado de protección de datos en los términos previstos en el artículo 40 o no posibilitar la efectiva participación del mismo en todas las cuestiones relativas a la protección de datos personales, no respaldarlo o interferir en el desempeño de sus funciones.

e) El incumplimiento de la puesta a disposición al interesado de la información prevista en el artículo 21 o del deber de comunicación al mismo, o a la autoridad de protección de datos competente, de una violación de la seguridad de los datos, que entrañe un grave perjuicio para los derechos y libertades del interesado.

f) La ausencia de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para aplicar de forma efectiva los principios de protección de datos, incluidas las medidas oportunas desde el diseño y por defecto, así como para integrar las garantías necesarias en el tratamiento.

g) El impedimento, la falta de atención o la obstaculización de los derechos del interesado de acceso, rectificación, supresión de sus datos o limitación del tratamiento, siempre que no constituya infracción muy grave.

h) El incumplimiento de la obligación de llevanza de los registros de actividades de tratamiento o del registro de operaciones de tratamiento, si se causan perjuicios de carácter grave a los interesados.

i) El incumplimiento de las estipulaciones recogidas en el contrato u acto jurídico que vincula al responsable y al encargado del tratamiento, salvo en los supuestos en que fuese necesario para evitar la infracción de la legislación en materia de protección de datos y se hubiese advertido de ello al responsable o al encargado del tratamiento, así como el incumplimiento de las obligaciones impuestas en el artículo 30.

j) La falta de colaboración diligente con las autoridades competentes en el cumplimiento de las obligaciones establecidas en el artículo 7, cuando no constituya una infracción muy grave.

k) La falta de cooperación, la actuación negligente o el impedimento de la función inspectora de las autoridades de protección de datos competentes, cuando no constituya infracción muy grave.

l) El incumplimiento de la evaluación de impacto en la protección de los datos de carácter personal, si se derivan perjuicios o riesgos de carácter grave para los interesados.

m) El tratamiento de datos personales sin haber consultado previamente a la autoridad de protección de datos competente, en los casos en que dicha consulta resulte preceptiva conforme al artículo 36.

Artículo 60. *Infracciones leves.*

Son infracciones leves:

a) La afectación leve de los derechos de los interesados como consecuencia de la ausencia de la debida diligencia o del carácter inadecuado o insuficiente de las medidas técnicas y organizativas que se hubiesen implantado.

b) El incumplimiento del principio de transparencia de la información o del derecho de información del interesado establecido en el artículo 21 cuando no se facilite toda la información exigida en esta Ley Orgánica.

c) La inobservancia de la obligación de informar al interesado y a los destinatarios a los que se hayan comunicado o de los que procedan los datos personales rectificados, suprimidos o respecto de los que se haya limitado el tratamiento, conforme a lo establecido en el artículo 23.

d) El incumplimiento de la llevanza de registros de actividades de tratamiento o del registro de operaciones o que los mismos no incorporen toda la información exigida legalmente, siempre que no constituya infracción grave.

e) El incumplimiento de la obligación de suprimir los datos referidos a una persona fallecida cuando fuera exigible legalmente.

f) La falta de formalización por los corresponsables del tratamiento del acuerdo que determine las obligaciones, funciones y responsabilidades respectivas, a propósito del tratamiento de datos personales y de sus relaciones con los interesados, así como la inexactitud o la falta de concreción en la determinación de las mismas.

g) El incumplimiento de la obligación del encargado del tratamiento de informar al responsable del tratamiento acerca de una posible infracción de las disposiciones de esta Ley Orgánica, como consecuencia de una instrucción recibida de este.

h) La notificación incompleta o defectuosa a la autoridad de protección de datos competente de la información relacionada con una violación de seguridad de los datos personales, el incumplimiento de la obligación de documentarla o del deber de comunicar al interesado su existencia, cuando no constituya una infracción grave.

i) La aportación de información inexacta o incompleta a la autoridad de protección de datos competente, en los supuestos en los que el responsable del tratamiento deba elevarle una consulta previa.

j) La falta de publicación de los datos de contacto del delegado de protección de datos, o la ausencia de comunicación de su designación y cese a la autoridad de protección de datos competente, de conformidad con el artículo 40, cuando su nombramiento sea exigible de acuerdo con esta Ley Orgánica.

Artículo 61. *Régimen jurídico.*

1. El ejercicio de la potestad sancionadora que corresponde a las autoridades de protección de datos competentes, se regirá por lo dispuesto en el presente capítulo, por los títulos VII y IX de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y, en cuanto no la contradiga, con carácter supletorio, por la normativa sobre el procedimiento administrativo común de las Administraciones Públicas y el régimen jurídico del sector público.

2. En el supuesto de las infracciones recogidas en los artículos 58. j) y 59. j), el ejercicio de la potestad sancionadora corresponderá respectivamente, a las personas titulares de la Secretaría de Estado de Seguridad y de las Delegaciones del Gobierno. Estos procedimientos se regirán por la normativa sobre procedimiento administrativo común de las Administraciones Públicas y el régimen jurídico del sector público, sin perjuicio de las especialidades que se recogen en este capítulo.

Artículo 62. *Sanciones.*

Por la comisión de las infracciones tipificadas en esta Ley Orgánica se impondrán las siguientes sanciones:

1. En caso de que el sujeto responsable sea algunos de los enumerados en el artículo 77.1 de la Ley Orgánica 3/2018, de 5 de diciembre, se impondrán las sanciones y se adoptarán las medidas establecidas en dicho artículo.

2. En caso de que el sujeto infractor sea distinto de los señalados en el artículo 77.1 de la Ley Orgánica 3/2018, de 5 de diciembre, podrá ser sancionado, con multa de la siguiente cuantía:

a) Las infracciones muy graves, con multa de 360.001 a 1.000.000 euros.
b) Las infracciones graves, con multa de 60.001 a 360.000 euros.
c) Las leves, con multa de 6.000 a 60.000 euros.

A efectos de la determinación de la cuantía de la sanción, se tendrán en cuenta los criterios establecidos en el artículo 83.2 del Reglamento General de Protección de Datos y en el artículo 76.2 de la Ley Orgánica 3/2018, de 5 de diciembre.

Artículo 63. *Prescripción de las infracciones y sanciones.*

1. Las infracciones administrativas tipificadas en esta Ley Orgánica prescribirán a los seis meses, a los dos o a los tres años de haberse cometido, según sean leves, graves o muy graves, respectivamente.

Los plazos señalados en esta Ley Orgánica se computarán desde el día en que se haya cometido la infracción. No obstante, en los casos de infracciones continuadas o permanentes, los plazos se computarán desde que finalizó la conducta infractora.

Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador, reiniciándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de seis meses por causas no imputables al presunto infractor.

Se interrumpirá igualmente la prescripción como consecuencia de la apertura de un procedimiento judicial penal, hasta que la autoridad judicial comunique al órgano administrativo su finalización.

2. Las sanciones impuestas por infracciones muy graves prescribirán a los tres años, las impuestas por infracciones graves, a los dos años, y las impuestas por infracciones leves al año, computados desde el día siguiente a aquel en que adquiera firmeza en vía administrativa la resolución por la que se impone la sanción.

La prescripción se interrumpirá por la iniciación, con conocimiento del interesado, del procedimiento de ejecución, volviendo a transcurrir el plazo si el mismo está paralizado durante más de seis meses por causa no imputable al infractor.

Artículo 64. *Caducidad del procedimiento.*

1. El procedimiento caducará transcurridos seis meses desde su incoación sin que se haya notificado la resolución, debiendo, no obstante, tenerse en cuenta en el cómputo las posibles paralizaciones por causas imputables al interesado o la suspensión que debiera acordarse por la existencia de un procedimiento judicial penal, cuando concurra identidad de sujeto, hecho y fundamento, hasta la finalización de este.

2. La resolución que declare la caducidad se notificará al interesado y pondrá fin al procedimiento, sin perjuicio de que la administración pueda acordar la incoación de un nuevo procedimiento en tanto no haya prescrito la infracción. Los procedimientos caducados no interrumpirán el plazo de prescripción.

Artículo 65. *Carácter subsidiario del procedimiento administrativo sancionador respecto del penal.*

1. No podrán sancionarse los hechos que hayan sido sancionados penal o administrativamente cuando se aprecie identidad de sujeto, de hecho y de fundamento.

2. En los supuestos en que las conductas pudieran ser constitutivas de delito, el órgano administrativo pasará el tanto de culpa a la autoridad judicial o al Ministerio Fiscal y se abstendrá de seguir el procedimiento sancionador mientras la autoridad judicial no dicte sentencia firme o resolución que de otro modo ponga fin al procedimiento penal, o el Ministerio Fiscal no acuerde la improcedencia de iniciar o proseguir las actuaciones en vía penal, quedando hasta entonces interrumpido el plazo de prescripción.

La autoridad judicial y el Ministerio Fiscal comunicarán al órgano administrativo la resolución o acuerdo que hubieran adoptado.

3. De no haberse estimado la existencia de ilícito penal, o en el caso de haberse dictado resolución de otro tipo que ponga fin al procedimiento penal, podrá iniciarse o proseguir el procedimiento sancionador. En todo caso, el órgano administrativo quedará vinculado por los hechos declarados probados en vía judicial.

4. Las medidas cautelares adoptadas antes de la intervención judicial podrán mantenerse mientras la autoridad judicial no resuelva otra cosa.

Disposición adicional primera. *Regímenes específicos.*

1. El tratamiento de los datos personales procedentes de las imágenes y sonidos obtenidos mediante la utilización de cámaras y videocámaras por las Fuerzas y Cuerpos de Seguridad, por los órganos competentes para la vigilancia y control en los centros penitenciarios y para el control, regulación, vigilancia y disciplina del tráfico, para los fines previstos en al artículo 1, se regirá por esta Ley Orgánica, sin perjuicio de los requisitos establecidos en regímenes legales especiales que regulan otros ámbitos concretos como el procesal penal, la regulación del tráfico o la protección de instalaciones propias.

2. Fuera de estos supuestos, dichos tratamientos se regirán por su legislación específica y supletoriamente por el Reglamento (UE) 2016/679 y por la Ley Orgánica 3/2018, de 5 de diciembre.

Disposición adicional segunda. *Intercambio de datos dentro de la Unión Europea.*

El intercambio de datos personales por parte de las autoridades competentes españolas en el interior de la Unión Europea, cuando el Derecho de la Unión Europea o la legislación española exijan dicho intercambio, no estará limitado ni prohibido por motivos relacionados con la protección de las personas físicas respecto al tratamiento de sus datos personales.

Disposición adicional tercera. *Acuerdos internacionales en el ámbito de la cooperación judicial en materia penal y de la cooperación policial.*

Los acuerdos internacionales en el ámbito de la cooperación judicial en materia penal y de la cooperación policial que impliquen la transferencia de datos personales a Estados que no sean miembros de la Unión Europea u organizaciones internacionales y que hubieran sido celebrados por España antes del 6 de mayo de 2016, cumpliendo lo dispuesto en el

Derecho de la Unión Europea aplicable antes de dicha fecha, seguirán en vigor hasta que sean objeto de modificación, enmienda o terminación.

Disposición adicional cuarta. *Ficheros y Registro de Población de las Administraciones Públicas.*

1. Las autoridades competentes podrán solicitar al Instituto Nacional de Estadística y a los órganos estadísticos de ámbito autonómico, sin consentimiento del interesado, una copia actualizada del fichero formado con los datos del documento de identidad, nombre, apellidos, domicilio, sexo y fecha de nacimiento que constan en el padrón municipal de habitantes y en el censo electoral correspondiente a los territorios donde ejerzan sus competencias. Esta solicitud deberá estar motivada en base a cualquiera de los fines de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública.

2. Los datos obtenidos tendrán como único propósito el cumplimiento de los fines de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, así como de protección y de prevención frente a las amenazas contra la seguridad pública y la comunicación de estas autoridades con los interesados residentes en los respectivos territorios, respecto a las relaciones jurídico-administrativas derivadas de las competencias respectivas.

Disposición adicional quinta. *Referencias normativas.*

Las referencias contenidas en normas vigentes en relación a las disposiciones que se derogan expresamente, deberán entenderse efectuadas a los artículos de esta Ley Orgánica que regulan la misma materia que aquellas.

Disposición transitoria única. *Duración del mandato inicial de la persona titular de la Dirección de Supervisión y Control de Protección de datos del Consejo General del Poder Judicial.*

La duración del mandato del primer nombramiento de la persona titular de la Dirección de Supervisión y Control de Protección de datos del Consejo General del Poder Judicial será de tres años no renovable.

Disposición derogatoria única. *Derogación normativa.*

Quedan derogadas todas las normas de igual o inferior rango en lo que contradigan o se opongan a lo dispuesto en esta Ley Orgánica.

[. . .]

Disposición final novena. *Naturaleza de la ley.*

Esta ley tiene el carácter de Ley Orgánica. No obstante, tienen carácter ordinario:

a) El capítulo VI.
b) El capítulo VII.
c) El capítulo VIII.
d) Las disposiciones finales segunda, sexta, séptima y octava.

Disposición final décima. *Título competencial.*

Esta Ley Orgánica se dicta al amparo de las reglas 1.ª, 6.ª, 18.ª y 29.ª del artículo 149.1 de la Constitución, que atribuyen al Estado las competencias exclusivas, respectivamente, para la regulación de las condiciones básicas que garanticen la igualdad de todos los españoles en el ejercicio de los derechos y en el cumplimiento de los deberes constitucionales; respecto a las bases del régimen jurídico de las Administraciones Públicas, el procedimiento administrativo común y en relación al sistema de responsabilidad de todas las Administraciones públicas; sobre legislación penal, penitenciaria, procesal; y en materia de seguridad pública.

Disposición final undécima. *Incorporación del Derecho de la Unión Europea.*

Mediante esta Ley Orgánica se incorpora al ordenamiento jurídico español la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

Disposición final duodécima. *Entrada en vigor.*

Esta Ley Orgánica entrará en vigor a los veinte días de su publicación en el «Boletín Oficial del Estado».

No obstante, las previsiones contenidas en el capítulo IV producirán efectos a los seis meses de la entrada en vigor de la Ley Orgánica.

§ 55

Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 236, de 2 de octubre de 2015
Última modificación: 6 de noviembre de 2024
Referencia: BOE-A-2015-10565

[. . .]

TÍTULO II

De la actividad de las Administraciones Públicas

CAPÍTULO I

Normas generales de actuación

Artículo 13. *Derechos de las personas en sus relaciones con las Administraciones Públicas.*

Quienes de conformidad con el artículo 3, tienen capacidad de obrar ante las Administraciones Públicas, son titulares, en sus relaciones con ellas, de los siguientes derechos:

a) A comunicarse con las Administraciones Públicas a través de un Punto de Acceso General electrónico de la Administración.

b) A ser asistidos en el uso de medios electrónicos en sus relaciones con las Administraciones Públicas.

c) A utilizar las lenguas oficiales en el territorio de su Comunidad Autónoma, de acuerdo con lo previsto en esta Ley y en el resto del ordenamiento jurídico.

d) Al acceso a la información pública, archivos y registros, de acuerdo con lo previsto en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno y el resto del Ordenamiento Jurídico.

e) A ser tratados con respeto y deferencia por las autoridades y empleados públicos, que habrán de facilitarles el ejercicio de sus derechos y el cumplimiento de sus obligaciones.

f) A exigir las responsabilidades de las Administraciones Públicas y autoridades, cuando así corresponda legalmente.

g) A la obtención y utilización de los medios de identificación y firma electrónica contemplados en esta Ley.

h) A la protección de datos de carácter personal, y en particular a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.

i) Cualesquiera otros que les reconozcan la Constitución y las leyes.

Estos derechos se entienden sin perjuicio de los reconocidos en el artículo 53 referidos a los interesados en el procedimiento administrativo.

[. . .]

Artículo 16. *Registros.*

1. Cada Administración dispondrá de un Registro Electrónico General, en el que se hará el correspondiente asiento de todo documento que sea presentado o que se reciba en cualquier órgano administrativo, Organismo público o Entidad vinculado o dependiente a éstos. También se podrán anotar en el mismo, la salida de los documentos oficiales dirigidos a otros órganos o particulares.

Los Organismos públicos vinculados o dependientes de cada Administración podrán disponer de su propio registro electrónico plenamente interoperable e interconectado con el Registro Electrónico General de la Administración de la que depende.

El Registro Electrónico General de cada Administración funcionará como un portal que facilitará el acceso a los registros electrónicos de cada Organismo. Tanto el Registro Electrónico General de cada Administración como los registros electrónicos de cada Organismo cumplirán con las garantías y medidas de seguridad previstas en la legislación en materia de protección de datos de carácter personal.

Las disposiciones de creación de los registros electrónicos se publicarán en el diario oficial correspondiente y su texto íntegro deberá estar disponible para consulta en la sede electrónica de acceso al registro. En todo caso, las disposiciones de creación de registros electrónicos especificarán el órgano o unidad responsable de su gestión, así como la fecha y hora oficial y los días declarados como inhábiles.

En la sede electrónica de acceso a cada registro figurará la relación actualizada de trámites que pueden iniciarse en el mismo.

2. Los asientos se anotarán respetando el orden temporal de recepción o salida de los documentos, e indicarán la fecha del día en que se produzcan. Concluido el trámite de registro, los documentos serán cursados sin dilación a sus destinatarios y a las unidades administrativas correspondientes desde el registro en que hubieran sido recibidas.

3. El registro electrónico de cada Administración u Organismo garantizará la constancia, en cada asiento que se practique, de un número, epígrafe expresivo de su naturaleza, fecha y hora de su presentación, identificación del interesado, órgano administrativo remitente, si procede, y persona u órgano administrativo al que se envía, y, en su caso, referencia al contenido del documento que se registra. Para ello, se emitirá automáticamente un recibo consistente en una copia autenticada del documento de que se trate, incluyendo la fecha y hora de presentación y el número de entrada de registro, así como un recibo acreditativo de otros documentos que, en su caso, lo acompañen, que garantice la integridad y el no repudio de los mismos.

4. Los documentos que los interesados dirijan a los órganos de las Administraciones Públicas podrán presentarse:

a) En el registro electrónico de la Administración u Organismo al que se dirijan, así como en los restantes registros electrónicos de cualquiera de los sujetos a los que se refiere el artículo 2.1.

b) En las oficinas de Correos, en la forma que reglamentariamente se establezca.

c) En las representaciones diplomáticas u oficinas consulares de España en el extranjero.

d) En las oficinas de asistencia en materia de registros.

e) En cualquier otro que establezcan las disposiciones vigentes.

Los registros electrónicos de todas y cada una de las Administraciones, deberán ser plenamente interoperables, de modo que se garantice su compatibilidad informática e interconexión, así como la transmisión telemática de los asientos registrales y de los documentos que se presenten en cualquiera de los registros.

5. Los documentos presentados de manera presencial ante las Administraciones Públicas, deberán ser digitalizados, de acuerdo con lo previsto en el artículo 27 y demás normativa aplicable, por la oficina de asistencia en materia de registros en la que hayan sido

presentados para su incorporación al expediente administrativo electrónico, devolviéndose los originales al interesado, sin perjuicio de aquellos supuestos en que la norma determine la custodia por la Administración de los documentos presentados o resulte obligatoria la presentación de objetos o de documentos en un soporte específico no susceptibles de digitalización.

Reglamentariamente, las Administraciones podrán establecer la obligación de presentar determinados documentos por medios electrónicos para ciertos procedimientos y colectivos de personas físicas que, por razón de su capacidad económica, técnica, dedicación profesional u otros motivos quede acreditado que tienen acceso y disponibilidad de los medios electrónicos necesarios.

6. Podrán hacerse efectivos mediante transferencia dirigida a la oficina pública correspondiente cualesquiera cantidades que haya que satisfacer en el momento de la presentación de documentos a las Administraciones Públicas, sin perjuicio de la posibilidad de su abono por otros medios.

7. Las Administraciones Públicas deberán hacer pública y mantener actualizada una relación de las oficinas en las que se prestará asistencia para la presentación electrónica de documentos.

8. No se tendrán por presentados en el registro aquellos documentos e información cuyo régimen especial establezca otra forma de presentación.

Artículo 17. *Archivo de documentos.*

1. Cada Administración deberá mantener un archivo electrónico único de los documentos electrónicos que correspondan a procedimientos finalizados, en los términos establecidos en la normativa reguladora aplicable.

2. Los documentos electrónicos deberán conservarse en un formato que permita garantizar la autenticidad, integridad y conservación del documento, así como su consulta con independencia del tiempo transcurrido desde su emisión. Se asegurará en todo caso la posibilidad de trasladar los datos a otros formatos y soportes que garanticen el acceso desde diferentes aplicaciones. La eliminación de dichos documentos deberá ser autorizada de acuerdo a lo dispuesto en la normativa aplicable.

3. Los medios o soportes en que se almacenen documentos, deberán contar con medidas de seguridad, de acuerdo con lo previsto en el Esquema Nacional de Seguridad, que garanticen la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados. En particular, asegurarán la identificación de los usuarios y el control de accesos, así como el cumplimiento de las garantías previstas en la legislación de protección de datos.

[. . .]

Artículo 20. *Responsabilidad de la tramitación.*

1. Los titulares de las unidades administrativas y el personal al servicio de las Administraciones Públicas que tuviesen a su cargo la resolución o el despacho de los asuntos, serán responsables directos de su tramitación y adoptarán las medidas oportunas para remover los obstáculos que impidan, dificulten o retrasen el ejercicio pleno de los derechos de los interesados o el respeto a sus intereses legítimos, disponiendo lo necesario para evitar y eliminar toda anormalidad en la tramitación de procedimientos.

2. Los interesados podrán solicitar la exigencia de esa responsabilidad a la Administración Pública de que dependa el personal afectado.

[. . .]

Artículo 27. *Validez y eficacia de las copias realizadas por las Administraciones Públicas.*

1. Cada Administración Pública determinará los órganos que tengan atribuidas las competencias de expedición de copias auténticas de los documentos públicos administrativos o privados.

Las copias auténticas de documentos privados surten únicamente efectos administrativos. Las copias auténticas realizadas por una Administración Pública tendrán validez en las restantes Administraciones.

A estos efectos, la Administración General del Estado, las Comunidades Autónomas y las Entidades Locales podrán realizar copias auténticas mediante funcionario habilitado o mediante actuación administrativa automatizada.

Se deberá mantener actualizado un registro, u otro sistema equivalente, donde constarán los funcionarios habilitados para la expedición de copias auténticas que deberán ser plenamente interoperables y estar interconectados con los de las restantes Administraciones Públicas, a los efectos de comprobar la validez de la citada habilitación. En este registro o sistema equivalente constarán, al menos, los funcionarios que presten servicios en las oficinas de asistencia en materia de registros.

2. Tendrán la consideración de copia auténtica de un documento público administrativo o privado las realizadas, cualquiera que sea su soporte, por los órganos competentes de las Administraciones Públicas en las que quede garantizada la identidad del órgano que ha realizado la copia y su contenido.

Las copias auténticas tendrán la misma validez y eficacia que los documentos originales.

3. Para garantizar la identidad y contenido de las copias electrónicas o en papel, y por tanto su carácter de copias auténticas, las Administraciones Públicas deberán ajustarse a lo previsto en el Esquema Nacional de Interoperabilidad, el Esquema Nacional de Seguridad y sus normas técnicas de desarrollo, así como a las siguientes reglas:

a) Las copias electrónicas de un documento electrónico original o de una copia electrónica auténtica, con o sin cambio de formato, deberán incluir los metadatos que acrediten su condición de copia y que se visualicen al consultar el documento.

b) Las copias electrónicas de documentos en soporte papel o en otro soporte no electrónico susceptible de digitalización, requerirán que el documento haya sido digitalizado y deberán incluir los metadatos que acrediten su condición de copia y que se visualicen al consultar el documento.

Se entiende por digitalización, el proceso tecnológico que permite convertir un documento en soporte papel o en otro soporte no electrónico en un fichero electrónico que contiene la imagen codificada, fiel e íntegra del documento.

c) Las copias en soporte papel de documentos electrónicos requerirán que en las mismas figure la condición de copia y contendrán un código generado electrónicamente u otro sistema de verificación, que permitirá contrastar la autenticidad de la copia mediante el acceso a los archivos electrónicos del órgano u Organismo público emisor.

d) Las copias en soporte papel de documentos originales emitidos en dicho soporte se proporcionarán mediante una copia auténtica en papel del documento electrónico que se encuentre en poder de la Administración o bien mediante una puesta de manifiesto electrónica conteniendo copia auténtica del documento original.

A estos efectos, las Administraciones harán públicos, a través de la sede electrónica correspondiente, los códigos seguros de verificación u otro sistema de verificación utilizado.

4. Los interesados podrán solicitar, en cualquier momento, la expedición de copias auténticas de los documentos públicos administrativos que hayan sido válidamente emitidos por las Administraciones Públicas. La solicitud se dirigirá al órgano que emitió el documento original, debiendo expedirse, salvo las excepciones derivadas de la aplicación de la Ley 19/2013, de 9 de diciembre, en el plazo de quince días a contar desde la recepción de la solicitud en el registro electrónico de la Administración u Organismo competente.

Asimismo, las Administraciones Públicas estarán obligadas a expedir copias auténticas electrónicas de cualquier documento en papel que presenten los interesados y que se vaya a incorporar a un expediente administrativo.

5. Cuando las Administraciones Públicas expidan copias auténticas electrónicas, deberá quedar expresamente así indicado en el documento de la copia.

6. La expedición de copias auténticas de documentos públicos notariales, registrales y judiciales, así como de los diarios oficiales, se regirá por su legislación específica.

Artículo 28. *Documentos aportados por los interesados al procedimiento administrativo.*

1. Los interesados deberán aportar al procedimiento administrativo los datos y documentos exigidos por las Administraciones Públicas de acuerdo con lo dispuesto en la normativa aplicable. Asimismo, los interesados podrán aportar cualquier otro documento que estimen conveniente.

2. Los interesados tienen derecho a no aportar documentos que ya se encuentren en poder de la Administración actuante o hayan sido elaborados por cualquier otra Administración. La administración actuante podrá consultar o recabar dichos documentos salvo que el interesado se opusiera a ello. No cabrá la oposición cuando la aportación del documento se exigiera en el marco del ejercicio de potestades sancionadoras o de inspección.

Las Administraciones Públicas deberán recabar los documentos electrónicamente a través de sus redes corporativas o mediante consulta a las plataformas de intermediación de datos u otros sistemas electrónicos habilitados al efecto.

Cuando se trate de informes preceptivos ya elaborados por un órgano administrativo distinto al que tramita el procedimiento, estos deberán ser remitidos en el plazo de diez días a contar desde su solicitud. Cumplido este plazo, se informará al interesado de que puede aportar este informe o esperar a su remisión por el órgano competente.

3. Las Administraciones no exigirán a los interesados la presentación de documentos originales, salvo que, con carácter excepcional, la normativa reguladora aplicable establezca lo contrario.

Asimismo, las Administraciones Públicas no requerirán a los interesados datos o documentos no exigidos por la normativa reguladora aplicable o que hayan sido aportados anteriormente por el interesado a cualquier Administración. A estos efectos, el interesado deberá indicar en qué momento y ante qué órgano administrativo presentó los citados documentos, debiendo las Administraciones Públicas recabarlos electrónicamente a través de sus redes corporativas o de una consulta a las plataformas de intermediación de datos u otros sistemas electrónicos habilitados al efecto, salvo que conste en el procedimiento la oposición expresa del interesado o la ley especial aplicable requiera su consentimiento expreso. Excepcionalmente, si las Administraciones Públicas no pudieran recabar los citados documentos, podrán solicitar nuevamente al interesado su aportación.

4. Cuando con carácter excepcional, y de acuerdo con lo previsto en esta Ley, la Administración solicitara al interesado la presentación de un documento original y éste estuviera en formato papel, el interesado deberá obtener una copia auténtica, según los requisitos establecidos en el artículo 27, con carácter previo a su presentación electrónica. La copia electrónica resultante reflejará expresamente esta circunstancia.

5. Excepcionalmente, cuando la relevancia del documento en el procedimiento lo exija o existan dudas derivadas de la calidad de la copia, las Administraciones podrán solicitar de manera motivada el cotejo de las copias aportadas por el interesado, para lo que podrán requerir la exhibición del documento o de la información original.

6. Las copias que aporten los interesados al procedimiento administrativo tendrán eficacia, exclusivamente en el ámbito de la actividad de las Administraciones Públicas.

7. Los interesados se responsabilizarán de la veracidad de los documentos que presenten.

CAPÍTULO II

Términos y plazos

[. . .]

Artículo 31. *Cómputo de plazos en los registros.*

1. Cada Administración Pública publicará los días y el horario en el que deban permanecer abiertas las oficinas que prestarán asistencia para la presentación electrónica de documentos, garantizando el derecho de los interesados a ser asistidos en el uso de medios electrónicos.

2. El registro electrónico de cada Administración u Organismo se regirá a efectos de cómputo de los plazos, por la fecha y hora oficial de la sede electrónica de acceso, que deberá contar con las medidas de seguridad necesarias para garantizar su integridad y figurar de modo accesible y visible.

El funcionamiento del registro electrónico se regirá por las siguientes reglas:

a) Permitirá la presentación de documentos todos los días del año durante las veinticuatro horas.

b) A los efectos del cómputo de plazo fijado en días hábiles, y en lo que se refiere al cumplimiento de plazos por los interesados, la presentación en un día inhábil se entenderá realizada en la primera hora del primer día hábil siguiente salvo que una norma permita expresamente la recepción en día inhábil.

Los documentos se considerarán presentados por el orden de hora efectiva en el que lo fueron en el día inhábil. Los documentos presentados en el día inhábil se reputarán anteriores, según el mismo orden, a los que lo fueran el primer día hábil posterior.

c) El inicio del cómputo de los plazos que hayan de cumplir las Administraciones Públicas vendrá determinado por la fecha y hora de presentación en el registro electrónico de cada Administración u Organismo. En todo caso, la fecha y hora efectiva de inicio del cómputo de plazos deberá ser comunicada a quien presentó el documento.

3. La sede electrónica del registro de cada Administración Pública u Organismo, determinará, atendiendo al ámbito territorial en el que ejerce sus competencias el titular de aquélla y al calendario previsto en el artículo 30.7, los días que se considerarán inhábiles a los efectos previstos en este artículo. Este será el único calendario de días inhábiles que se aplicará a efectos del cómputo de plazos en los registros electrónicos, sin que resulte de aplicación a los mismos lo dispuesto en el artículo 30.6.

Artículo 32. *Ampliación.*

1. La Administración, salvo precepto en contrario, podrá conceder de oficio o a petición de los interesados, una ampliación de los plazos establecidos, que no exceda de la mitad de los mismos, si las circunstancias lo aconsejan y con ello no se perjudican derechos de tercero. El acuerdo de ampliación deberá ser notificado a los interesados.

2. La ampliación de los plazos por el tiempo máximo permitido se aplicará en todo caso a los procedimientos tramitados por las misiones diplomáticas y oficinas consulares, así como a aquellos que, sustanciándose en el interior, exijan cumplimentar algún trámite en el extranjero o en los que intervengan interesados residentes fuera de España.

3. Tanto la petición de los interesados como la decisión sobre la ampliación deberán producirse, en todo caso, antes del vencimiento del plazo de que se trate. En ningún caso podrá ser objeto de ampliación un plazo ya vencido. Los acuerdos sobre ampliación de plazos o sobre su denegación no serán susceptibles de recurso, sin perjuicio del procedente contra la resolución que ponga fin al procedimiento.

4. Cuando una incidencia técnica haya imposibilitado el funcionamiento ordinario del sistema o aplicación que corresponda, y hasta que se solucione el problema, la Administración podrá determinar una ampliación de los plazos no vencidos, debiendo publicar en la sede electrónica tanto la incidencia técnica acontecida como la ampliación concreta del plazo no vencido.

5. Cuando como consecuencia de un ciberincidente se hayan visto gravemente afectados los servicios y sistemas utilizados para la tramitación de los procedimientos y el ejercicio de los derechos de los interesados que prevé la normativa vigente, la Administración podrá acordar la ampliación general de plazos de los procedimientos administrativos.

[. . .]

TÍTULO III

De los actos administrativos

[. . .]

CAPÍTULO II

Eficacia de los actos

[. . .]

Artículo 40. *Notificación.*

1. El órgano que dicte las resoluciones y actos administrativos los notificará a los interesados cuyos derechos e intereses sean afectados por aquéllos, en los términos previstos en los artículos siguientes.

2. Toda notificación deberá ser cursada dentro del plazo de diez días a partir de la fecha en que el acto haya sido dictado, y deberá contener el texto íntegro de la resolución, con indicación de si pone fin o no a la vía administrativa, la expresión de los recursos que procedan, en su caso, en vía administrativa y judicial, el órgano ante el que hubieran de presentarse y el plazo para interponerlos, sin perjuicio de que los interesados puedan ejercitar, en su caso, cualquier otro que estimen procedente.

3. Las notificaciones que, conteniendo el texto íntegro del acto, omitiesen alguno de los demás requisitos previstos en el apartado anterior, surtirán efecto a partir de la fecha en que el interesado realice actuaciones que supongan el conocimiento del contenido y alcance de la resolución o acto objeto de la notificación, o interponga cualquier recurso que proceda.

4. Sin perjuicio de lo establecido en el apartado anterior, y a los solos efectos de entender cumplida la obligación de notificar dentro del plazo máximo de duración de los procedimientos, será suficiente la notificación que contenga, cuando menos, el texto íntegro de la resolución, así como el intento de notificación debidamente acreditado.

5. Las Administraciones Públicas podrán adoptar las medidas que consideren necesarias para la protección de los datos personales que consten en las resoluciones y actos administrativos, cuando éstos tengan por destinatarios a más de un interesado.

[. . .]

TÍTULO IV

De las disposiciones sobre el procedimiento administrativo común

[. . .]

CAPÍTULO III

Ordenación del procedimiento

Artículo 70. *Expediente Administrativo.*

1. Se entiende por expediente administrativo el conjunto ordenado de documentos y actuaciones que sirven de antecedente y fundamento a la resolución administrativa, así como las diligencias encaminadas a ejecutarla.

2. Los expedientes tendrán formato electrónico y se formarán mediante la agregación ordenada de cuantos documentos, pruebas, dictámenes, informes, acuerdos, notificaciones y demás diligencias deban integrarlos, así como un índice numerado de todos los documentos que contenga cuando se remita. Asimismo, deberá constar en el expediente copia electrónica certificada de la resolución adoptada.

3. Cuando en virtud de una norma sea preciso remitir el expediente electrónico, se hará de acuerdo con lo previsto en el Esquema Nacional de Interoperabilidad y en las correspondientes Normas Técnicas de Interoperabilidad, y se enviará completo, foliado, autentificado y acompañado de un índice, asimismo autentificado, de los documentos que contenga. La autenticación del citado índice garantizará la integridad e inmutabilidad del

expediente electrónico generado desde el momento de su firma y permitirá su recuperación siempre que sea preciso, siendo admisible que un mismo documento forme parte de distintos expedientes electrónicos.

4. No formará parte del expediente administrativo la información que tenga carácter auxiliar o de apoyo, como la contenida en aplicaciones, ficheros y bases de datos informáticas, notas, borradores, opiniones, resúmenes, comunicaciones e informes internos o entre órganos o entidades administrativas, así como los juicios de valor emitidos por las Administraciones Públicas, salvo que se trate de informes, preceptivos y facultativos, solicitados antes de la resolución administrativa que ponga fin al procedimiento.

[. . .]

Disposición adicional segunda. *Adhesión de las Comunidades Autónomas y Entidades Locales a las plataformas y registros de la Administración General del Estado.*

Para cumplir con lo previsto en materia de registro electrónico de apoderamientos, registro electrónico, archivo electrónico único, plataforma de intermediación de datos y punto de acceso general electrónico de la Administración, las Comunidades Autónomas y las Entidades Locales podrán adherirse voluntariamente y a través de medios electrónicos a las plataformas y registros establecidos al efecto por la Administración General del Estado. Su no adhesión, deberá justificarse en términos de eficiencia conforme al artículo 7 de la Ley Orgánica 2/2012, de 27 de abril, de Estabilidad Presupuestaria y Sostenibilidad Financiera.

En el caso que una Comunidad Autónoma o una Entidad Local justifique ante el Ministerio de Hacienda y Administraciones Públicas que puede prestar el servicio de un modo más eficiente, de acuerdo con los criterios previstos en el párrafo anterior, y opte por mantener su propio registro o plataforma, las citadas Administraciones deberán garantizar que éste cumple con los requisitos del Esquema Nacional de Interoperabilidad, el Esquema Nacional de Seguridad, y sus normas técnicas de desarrollo, de modo que se garantice su compatibilidad informática e interconexión, así como la transmisión telemática de las solicitudes, escritos y comunicaciones que se realicen en sus correspondientes registros y plataformas.

Téngase en cuenta que se declara que el párrafo segundo no es inconstitucional interpretado en los términos del fundamento jurídico 11 f) por Sentencia del TC 55/2018, de 24 de mayo. Ref. BOE-A-2018-8574

[. . .]

Disposición adicional octava. *Resoluciones de Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital que establezcan las condiciones de uso de sistemas de identificación y/o firma no criptográfica.*

Cuando se trate de sistemas establecidos por medio de Resolución de la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital para su ámbito competencial con objeto de determinar las circunstancias en las que un sistema de firma electrónica no basado en certificados electrónicos será considerado como válido en las relaciones de los interesados con los órganos administrativos de la Administración General del Estado, sus organismos públicos y entidades de Derecho Público vinculados o dependientes, no será preciso el transcurso del plazo de dos meses para la eficacia jurídica del sistema a que se refiere el artículo 10.2.c) de la presente ley, adquiriendo eficacia jurídica al día siguiente de la publicación de la Resolución, salvo que esta disponga otra cosa.

Disposición adicional novena. *Suspensión de plazos administrativos en los acuerdos de declaración de zonas afectadas gravemente por emergencias de protección civil.*

El acuerdo de Consejo de Ministros por el que se declare una zona afectada gravemente por una emergencia de protección civil, previsto en el artículo 23 de la Ley 17/2015, de 9 de julio, del Sistema Nacional de Protección Civil, podrá establecer la suspensión de los plazos para el cumplimiento de los trámites de los procedimientos administrativos del sector público que correspondan a los interesados residentes en los términos municipales incluidos en el ámbito de aplicación del acuerdo y, en su caso, a aquellos otros interesados que acrediten el carácter imposible o gravoso de su cumplimiento en atención a los efectos de la emergencia. La suspensión se mantendrá hasta el momento en que se dicte un nuevo acuerdo de Consejo de Ministros decretando la finalización de esta medida, tras lo cual se reanudarán los plazos suspendidos.

[. . .]

§ 56

Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 236, de 2 de octubre de 2015
Última modificación: 2 de agosto de 2024
Referencia: BOE-A-2015-10566

TÍTULO PRELIMINAR

Disposiciones generales, principios de actuación y funcionamiento del sector público

CAPÍTULO I

Disposiciones generales

[. . .]

Artículo 3. *Principios generales.*

1. Las Administraciones Públicas sirven con objetividad los intereses generales y actúan de acuerdo con los principios de eficacia, jerarquía, descentralización, desconcentración y coordinación, con sometimiento pleno a la Constitución, a la Ley y al Derecho.

Deberán respetar en su actuación y relaciones los siguientes principios:

a) Servicio efectivo a los ciudadanos.
b) Simplicidad, claridad y proximidad a los ciudadanos.
c) Participación, objetividad y transparencia de la actuación administrativa.
d) Racionalización y agilidad de los procedimientos administrativos y de las actividades materiales de gestión.
e) Buena fe, confianza legítima y lealtad institucional.
f) Responsabilidad por la gestión pública.
g) Planificación y dirección por objetivos y control de la gestión y evaluación de los resultados de las políticas públicas.
h) Eficacia en el cumplimiento de los objetivos fijados.
i) Economía, suficiencia y adecuación estricta de los medios a los fines institucionales.
j) Eficiencia en la asignación y utilización de los recursos públicos.
k) Cooperación, colaboración y coordinación entre las Administraciones Públicas.

2. Las Administraciones Públicas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos, que aseguren la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada

una de ellas, garantizarán la protección de los datos de carácter personal, y facilitarán preferentemente la prestación conjunta de servicios a los interesados.

3. Bajo la dirección del Gobierno de la Nación, de los órganos de gobierno de las Comunidades Autónomas y de los correspondientes de las Entidades Locales, la actuación de la Administración Pública respectiva se desarrolla para alcanzar los objetivos que establecen las leyes y el resto del ordenamiento jurídico.

4. Cada una de las Administraciones Públicas del artículo 2 actúa para el cumplimiento de sus fines con personalidad jurídica única.

Artículo 4. *Principios de intervención de las Administraciones Públicas para el desarrollo de una actividad.*

1. Las Administraciones Públicas que, en el ejercicio de sus respectivas competencias, establezcan medidas que limiten el ejercicio de derechos individuales o colectivos o exijan el cumplimiento de requisitos para el desarrollo de una actividad, deberán aplicar el principio de proporcionalidad y elegir la medida menos restrictiva, motivar su necesidad para la protección del interés público así como justificar su adecuación para lograr los fines que se persiguen, sin que en ningún caso se produzcan diferencias de trato discriminatorias. Asimismo deberán evaluar periódicamente los efectos y resultados obtenidos.

2. Las Administraciones Públicas velarán por el cumplimiento de los requisitos previstos en la legislación que resulte aplicable, para lo cual podrán, en el ámbito de sus respectivas competencias y con los límites establecidos en la legislación de protección de datos de carácter personal, comprobar, verificar, investigar e inspeccionar los hechos, actos, elementos, actividades, estimaciones y demás circunstancias que fueran necesarias.

CAPÍTULO II

De los órganos de las Administraciones Públicas

[. . .]

Sección 2.ª Competencia

[. . .]

Artículo 11. *Encomiendas de gestión.*

1. La realización de actividades de carácter material o técnico de la competencia de los órganos administrativos o de las Entidades de Derecho Público podrá ser encomendada a otros órganos o Entidades de Derecho Público de la misma o de distinta Administración, siempre que entre sus competencias estén esas actividades, por razones de eficacia o cuando no se posean los medios técnicos idóneos para su desempeño.

Las encomiendas de gestión no podrán tener por objeto prestaciones propias de los contratos regulados en la legislación de contratos del sector público. En tal caso, su naturaleza y régimen jurídico se ajustará a lo previsto en ésta.

2. La encomienda de gestión no supone cesión de la titularidad de la competencia ni de los elementos sustantivos de su ejercicio, siendo responsabilidad del órgano o Entidad encomendante dictar cuantos actos o resoluciones de carácter jurídico den soporte o en los que se integre la concreta actividad material objeto de encomienda.

En todo caso, la Entidad u órgano encomendado tendrá la condición de encargado del tratamiento de los datos de carácter personal a los que pudiera tener acceso en ejecución de la encomienda de gestión, siéndole de aplicación lo dispuesto en la normativa de protección de datos de carácter personal.

3. La formalización de las encomiendas de gestión se ajustará a las siguientes reglas:

a) Cuando la encomienda de gestión se realice entre órganos administrativos o Entidades de Derecho Público pertenecientes a la misma Administración deberá formalizarse en los términos que establezca su normativa propia y, en su defecto, por acuerdo expreso de los órganos o Entidades de Derecho Público intervinientes. En todo caso, el instrumento de formalización de la encomienda de gestión y su resolución deberá ser publicada, para su

eficacia, en el Boletín Oficial del Estado, en el Boletín oficial de la Comunidad Autónoma o en el de la Provincia, según la Administración a que pertenezca el órgano encomendante.

Cada Administración podrá regular los requisitos necesarios para la validez de tales acuerdos que incluirán, al menos, expresa mención de la actividad o actividades a las que afecten, el plazo de vigencia y la naturaleza y alcance de la gestión encomendada.

b) Cuando la encomienda de gestión se realice entre órganos y Entidades de Derecho Público de distintas Administraciones se formalizará mediante firma del correspondiente convenio entre ellas, que deberá ser publicado en el «Boletín Oficial del Estado», en el Boletín oficial de la Comunidad Autónoma o en el de la Provincia, según la Administración a que pertenezca el órgano encomendante, salvo en el supuesto de la gestión ordinaria de los servicios de las Comunidades Autónomas por las Diputaciones Provinciales o en su caso Cabildos o Consejos insulares, que se regirá por la legislación de Régimen Local.

[. . .]

CAPÍTULO V

Funcionamiento electrónico del sector público

Artículo 38. *La sede electrónica.*

1. La sede electrónica es aquella dirección electrónica, disponible para los ciudadanos a través de redes de telecomunicaciones, cuya titularidad corresponde a una Administración Pública, o bien a una o varios organismos públicos o entidades de Derecho Público en el ejercicio de sus competencias.

2. El establecimiento de una sede electrónica conlleva la responsabilidad del titular respecto de la integridad, veracidad y actualización de la información y los servicios a los que pueda accederse a través de la misma.

3. Cada Administración Pública determinará las condiciones e instrumentos de creación de las sedes electrónicas, con sujeción a los principios de transparencia, publicidad, responsabilidad, calidad, seguridad, disponibilidad, accesibilidad, neutralidad e interoperabilidad. En todo caso deberá garantizarse la identificación del órgano titular de la sede, así como los medios disponibles para la formulación de sugerencias y quejas.

4. Las sedes electrónicas dispondrán de sistemas que permitan el establecimiento de comunicaciones seguras siempre que sean necesarias.

5. La publicación en las sedes electrónicas de informaciones, servicios y transacciones respetará los principios de accesibilidad y uso de acuerdo con las normas establecidas al respecto, estándares abiertos y, en su caso, aquellos otros que sean de uso generalizado por los ciudadanos.

6. Las sedes electrónicas utilizarán, para identificarse y garantizar una comunicación segura con las mismas, certificados reconocidos o cualificados de autenticación de sitio web o medio equivalente.

[. . .]

Artículo 43. *Firma electrónica del personal al servicio de las Administraciones Públicas.*

1. Sin perjuicio de lo previsto en los artículos 38, 41 y 42, la actuación de una Administración Pública, órgano, organismo público o entidad de derecho público, cuando utilice medios electrónicos, se realizará mediante firma electrónica del titular del órgano o empleado público.

2. Cada Administración Pública determinará los sistemas de firma electrónica que debe utilizar su personal, los cuales podrán identificar de forma conjunta al titular del puesto de trabajo o cargo y a la Administración u órgano en la que presta sus servicios. Por razones de seguridad pública los sistemas de firma electrónica podrán referirse sólo el número de identificación profesional del empleado público.

Artículo 44. *Intercambio electrónico de datos en entornos cerrados de comunicación.*

1. Los documentos electrónicos transmitidos en entornos cerrados de comunicaciones establecidos entre Administraciones Públicas, órganos, organismos públicos y entidades de derecho público, serán considerados válidos a efectos de autenticación e identificación de los emisores y receptores en las condiciones establecidas en este artículo.

2. Cuando los participantes en las comunicaciones pertenezcan a una misma Administración Pública, ésta determinará las condiciones y garantías por las que se regirá que, al menos, comprenderá la relación de emisores y receptores autorizados y la naturaleza de los datos a intercambiar.

3. Cuando los participantes pertenezcan a distintas Administraciones, las condiciones y garantías citadas en el apartado anterior se establecerán mediante convenio suscrito entre aquellas.

4. En todo caso deberá garantizarse la seguridad del entorno cerrado de comunicaciones y la protección de los datos que se transmitan.

[. . .]

Artículo 46. *Archivo electrónico de documentos.*

1. Todos los documentos utilizados en las actuaciones administrativas se almacenarán por medios electrónicos, salvo cuando no sea posible.

2. Los documentos electrónicos que contengan actos administrativos que afecten a derechos o intereses de los particulares deberán conservarse en soportes de esta naturaleza, ya sea en el mismo formato a partir del que se originó el documento o en otro cualquiera que asegure la identidad e integridad de la información necesaria para reproducirlo. Se asegurará en todo caso la posibilidad de trasladar los datos a otros formatos y soportes que garanticen el acceso desde diferentes aplicaciones.

3. Los medios o soportes en que se almacenen documentos, deberán contar con medidas de seguridad, de acuerdo con lo previsto en el Esquema Nacional de Seguridad, que garanticen la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados. En particular, asegurarán la identificación de los usuarios y el control de accesos, el cumplimiento de las garantías previstas en la legislación de protección de datos, así como la recuperación y conservación a largo plazo de los documentos electrónicos producidos por las Administraciones Públicas que así lo requieran, de acuerdo con las especificaciones sobre el ciclo de vida de los servicios y sistemas utilizados.

Artículo 46 bis. *Ubicación de los sistemas de información y comunicaciones para el registro de datos.*

Los sistemas de información y comunicaciones para la recogida, almacenamiento, procesamiento y gestión del censo electoral, los padrones municipales de habitantes y otros registros de población, datos fiscales relacionados con tributos propios o cedidos y datos de los usuarios del sistema nacional de salud, así como los correspondientes tratamientos de datos personales, deberán ubicarse y prestarse dentro del territorio de la Unión Europea.

Los datos a que se refiere el apartado anterior no podrán ser objeto de transferencia a un tercer país u organización internacional, con excepción de los que hayan sido objeto de una decisión de adecuación de la Comisión Europea o cuando así lo exija el cumplimiento de las obligaciones internacionales asumidas por el Reino de España.

[. . .]

Artículo 55 bis. *Presencia equilibrada de mujeres y hombres en los órganos superiores y directivos de la Administración General del Estado.*

Las personas titulares de las Secretarías de Estado y de los órganos directivos de la Administración General del Estado se nombrarán atendiendo al principio de representación equilibrada entre mujeres y hombres, de tal manera que las personas de cada sexo no

superen el sesenta por ciento ni sean menos del cuarenta por ciento en el ámbito de cada departamento ministerial.

[. . .]

Artículo 84 bis. *Presencia equilibrada entre mujeres y hombres en las entidades del sector público institucional estatal.*

1. El principio de representación equilibrada entre mujeres y hombres será de aplicación a las personas titulares de las presidencias, vicepresidencias, direcciones generales, direcciones ejecutivas y asimilados de las entidades del sector público institucional estatal que tengan la condición de máximos responsables, así como a las personas con contratos de alta dirección en las citadas entidades, de tal manera que las personas de cada sexo no superen el sesenta por ciento ni sean menos del cuarenta por ciento en el ámbito de cada entidad.

2. El principio de representación equilibrada se garantizará también en la composición de los órganos colegiados de gobierno de las entidades.

[. . .]

TÍTULO III

Relaciones interadministrativas

[. . .]

CAPÍTULO IV

Relaciones electrónicas entre las Administraciones

Artículo 155. *Transmisiones de datos entre Administraciones Públicas.*

1. De conformidad con lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y su normativa de desarrollo, cada Administración deberá facilitar el acceso de las restantes Administraciones Públicas a los datos relativos a los interesados que obren en su poder, especificando las condiciones, protocolos y criterios funcionales o técnicos necesarios para acceder a dichos datos con las máximas garantías de seguridad, integridad y disponibilidad.

2. En ningún caso podrá procederse a un tratamiento ulterior de los datos para fines incompatibles con el fin para el cual se recogieron inicialmente los datos personales. De acuerdo con lo previsto en el artículo 5.1.b) del Reglamento (UE) 2016/679, no se considerará incompatible con los fines iniciales el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos.

3. Fuera del caso previsto en el apartado anterior y siempre que las leyes especiales aplicables a los respectivos tratamientos no prohíban expresamente el tratamiento ulterior de los datos para una finalidad distinta, cuando la Administración Pública cesionaria de los datos pretenda el tratamiento ulterior de los mismos para una finalidad que estime compatible con el fin inicial, deberá comunicarlo previamente a la Administración Pública cedente a los efectos de que esta pueda comprobar dicha compatibilidad. La Administración Pública cedente podrá, en el plazo de diez días oponerse motivadamente. Cuando la Administración cedente sea la Administración General del Estado podrá en este supuesto, excepcionalmente y de forma motivada, suspender la transmisión de datos por razones de seguridad nacional de forma cautelar por el tiempo estrictamente indispensable para su preservación. En tanto que la Administración Pública cedente no comunique su decisión a la cesionaria esta no podrá emplear los datos para la nueva finalidad pretendida.

Se exceptúan de lo dispuesto en el párrafo anterior los supuestos en que el tratamiento para otro fin distinto de aquel para el que se recogieron los datos personales esté previsto en una norma con rango de ley de conformidad con lo previsto en el artículo 23.1 del Reglamento (UE) 2016/679.

Artículo 156. *Esquema Nacional de Interoperabilidad y Esquema Nacional de Seguridad.*

1. El Esquema Nacional de Interoperabilidad comprende el conjunto de criterios y recomendaciones en materia de seguridad, conservación y normalización de la información, de los formatos y de las aplicaciones que deberán ser tenidos en cuenta por las Administraciones Públicas para la toma de decisiones tecnológicas que garanticen la interoperabilidad.

2. El Esquema Nacional de Seguridad tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la presente Ley, y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada.

Artículo 157. *Reutilización de sistemas y aplicaciones de propiedad de la Administración.*

1. Las Administraciones pondrán a disposición de cualquiera de ellas que lo solicite las aplicaciones, desarrolladas por sus servicios o que hayan sido objeto de contratación y de cuyos derechos de propiedad intelectual sean titulares, salvo que la información a la que estén asociadas sea objeto de especial protección por una norma. Las Administraciones cedentes y cesionarias podrán acordar la repercusión del coste de adquisición o fabricación de las aplicaciones cedidas.

2. Las aplicaciones a las que se refiere el apartado anterior podrán ser declaradas como de fuentes abiertas, cuando de ello se derive una mayor transparencia en el funcionamiento de la Administración Pública o se fomente con ello la incorporación de los ciudadanos a la Sociedad de la información.

3. Las Administraciones Públicas, con carácter previo a la adquisición, desarrollo o al mantenimiento a lo largo de todo el ciclo de vida de una aplicación, tanto si se realiza con medios propios o por la contratación de los servicios correspondientes, deberán consultar en el directorio general de aplicaciones, dependiente de la Administración General del Estado, si existen soluciones disponibles para su reutilización, que puedan satisfacer total o parcialmente las necesidades, mejoras o actualizaciones que se pretenden cubrir, y siempre que los requisitos tecnológicos de interoperabilidad y seguridad así lo permitan.

En este directorio constarán tanto las aplicaciones disponibles de la Administración General del Estado como las disponibles en los directorios integrados de aplicaciones del resto de Administraciones.

En el caso de existir una solución disponible para su reutilización total o parcial, las Administraciones Públicas estarán obligadas a su uso, salvo que la decisión de no reutilizarla se justifique en términos de eficiencia conforme al artículo 7 de la Ley Orgánica 2/2012, de 27 de abril, de Estabilidad Presupuestaria y Sostenibilidad Financiera.

Artículo 158. *Transferencia de tecnología entre Administraciones.*

1. Las Administraciones Públicas mantendrán directorios actualizados de aplicaciones para su libre reutilización, de conformidad con lo dispuesto en el Esquema Nacional de Interoperabilidad. Estos directorios deberán ser plenamente interoperables con el directorio general de la Administración General del Estado, de modo que se garantice su compatibilidad informática e interconexión.

2. La Administración General del Estado, mantendrá un directorio general de aplicaciones para su reutilización, prestará apoyo para la libre reutilización de aplicaciones e impulsará el desarrollo de aplicaciones, formatos y estándares comunes en el marco de los esquemas nacionales de interoperabilidad y seguridad.

[. . .]

Disposición adicional trigésima. *Plataforma Digital de Colaboración entre las Administraciones Públicas.*

1. El Ministerio de Asuntos Económicos y Transformación Digital y el Ministerio de Política Territorial impulsarán mediante orden ministerial conjunta las medidas necesarias para la creación y el funcionamiento de la Plataforma Digital de Colaboración entre las Administraciones Públicas como instrumento destinado a facilitar las relaciones y el soporte electrónico de los órganos integrantes del sistema de Conferencias Sectoriales y en general de los órganos de cooperación.

2. En aplicación del principio de colaboración, las Administraciones Públicas designarán los Puntos de Contacto correspondientes para atender las diversas funcionalidades de la Plataforma.

3. Reglamentariamente se regulará la configuración y régimen de funcionamiento de la Plataforma que, en cualquier caso, se adaptará a los criterios y directrices que sucesivamente establezca la Conferencia Sectorial de Administración Pública o, en su caso, la Comisión Sectorial de Administración Electrónica como órgano dependiente de aquélla.

[. . .]