Códigos electrónicos

Ámbitos de la Seguridad Nacional: Protección de Infraestructuras Críticas

Selección y ordenación:
Jorge Lozano Miralles
María José Carazo Liébana

Edición actualizada a 29 de enero de 2021

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

NIPO (PDF): 090-20-249-8
NIPO (Papel): 090-20-248-2
NIPO (ePUB): 090-20-250-0
ISBN: 978-84-340-2681-0
Depósito Legal: M-28053-2020

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

I. LEGISLACIÓN BÁSICA

II. COORDINACIÓN Y COOPERACIÓN PÚBLICO-PÚBLICO Y PÚBLICO-PRIVADA

Índice Sistemático

I. LEGISLACIÓN BÁSICA

II. COORDINACIÓN Y COOPERACIÓN PÚBLICO-PÚBLICO Y PÚBLICO-PRIVADA

§ 1

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.

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.

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.

§ 2

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».

§ 3

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: sin modificaciones
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.

d) Elaborar, según se disponga reglamentariamente, un Plan de Protección Específico por cada una de las infraestructuras consideradas como críticas en el Catálogo.

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.

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.

§ 4

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.

§ 5

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: 5 de noviembre de 2019
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 para el Avance Digital, del Ministerio de Economía y Empresa.

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.

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».

§ 6

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.

§ 7

Ley 5/2014, de 4 de abril, de Seguridad Privada. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 83, de 5 de abril de 2014
Última modificación: sin modificaciones
Referencia: BOE-A-2014-3649

TÍTULO II

Empresas de seguridad privada y despachos de detectives privados

CAPÍTULO I

Empresas de seguridad privada

[. . .]

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.

[. . .]

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.

[. . .]

TÍTULO IV

Servicios y medidas de seguridad

[. . .]

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.

[. . .]