I. DISPOSICIONES GENERALES

MINISTERIO DE TRABAJO Y ECONOMÍA SOCIAL

16757 *Orden TES/804/2026, de 23 de julio, por la que se aprueba la Política de Seguridad de la Información y de los Servicios en el ámbito de la administración digital del Ministerio de Trabajo y Economía Social y se crea el Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del departamento.*

La política de seguridad de la información es el conjunto de directrices que rigen la forma en que una entidad, en este caso, un departamento ministerial, gestiona y protege la información que trata y los servicios que presta.

En el ámbito del Ministerio de Trabajo y Economía Social se debe garantizar la seguridad como un proceso integral de cada etapa del ciclo de vida de cada sistema de información, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Además, el sistema de información debe estar preparado para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con lo que prevé el Esquema Nacional de Seguridad.

El marco de relación entre la Administración Pública y la ciudadanía a través de medios electrónicos se encuentra establecido en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. Asimismo, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público incorpora en su artículo 156 el Esquema Nacional de Seguridad como elemento esencial para garantizar la confianza en la actuación administrativa digital. Ambas normas fueron desarrolladas mediante el Reglamento de actuación y funcionamiento del sector público por medios electrónicos, aprobado por Real Decreto 203/2021, de 30 de marzo.

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, establece los principios y requisitos necesarios para garantizar la protección adecuada de la información y de los servicios públicos digitales, asegurando la confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y conservación de los datos, la información y los servicios utilizados por medios electrónicos que gestionen en el ejercicio de sus competencias. En particular su artículo 12.3 dispone que cada ministerio debe contar con su política de seguridad, aprobada por la persona titular del departamento.

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 adelante Reglamento General de Protección de Datos, señala que la protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos de dicho reglamento. A fin de poder demostrar la conformidad con el Reglamento General de Protección de Datos, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan, en particular, los principios de protección de datos desde el diseño y por defecto.

A tal efecto establece, en su artículo 24, como obligaciones generales del responsable del tratamiento y del encargado del tratamiento, la aplicación de las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el citado Reglamento General de Protección de Datos. Entre las medidas mencionadas se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas medidas para la protección de datos.

cve: BOE-A-2026-16757
Verificable en https://www.boe.es

Además de en el marco de las normas mencionadas con anterioridad, esta orden se dicta también de acuerdo con lo dispuesto en la disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos Digitales, que señala que, en el ámbito del sector público, el Esquema Nacional de Seguridad incluirá las medidas que deban implantarse en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento General de Protección de Datos, en orden a aplicar las medidas de seguridad al tratamiento de datos personales.

Con relación a la ciberseguridad, el Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones, incorpora medidas para la seguridad pública, asegurando aspectos relacionados con la mayor exposición a ciberamenazas que exigen una mejor protección de redes y sistemas, así como de la privacidad y los derechos digitales de las personas.

Respecto al marco normativo europeo, la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148, en adelante, Directiva NIS2, establece obligaciones de ciberseguridad para los Estados miembros, medidas para la gestión de riesgos de ciberseguridad y obligaciones de notificación para las entidades comprendidas en su ámbito de aplicación, así como obligaciones referentes al intercambio de información sobre ciberseguridad y obligaciones de supervisión y ejecución para los Estados miembros.

En cumplimiento del mandato previsto en el artículo 12.3 del Real Decreto 311/2022, de 3 de mayo, mediante la Orden TES/369/2023, de 10 de abril, por la que se aprueba la política de seguridad de la información y de los servicios en el ámbito de la administración digital del Ministerio de Trabajo y Economía Social y se crea el Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del departamento, se aprobó la primera política de seguridad de la información y de los servicios del Ministerio de Trabajo y Economía Social, creando el Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones. Sin embargo, la evolución normativa y tecnológica, las nuevas exigencias derivadas del Esquema Nacional de Seguridad, la incorporación de la vigilancia continua y la gestión dinámica del riesgo, así como la sucesiva reestructuración ministerial dada por los Reales Decretos 829/2023, de 20 de noviembre,1009/2023, de 5 de diciembre, y 502/2024, de 21 de mayo, hacen necesaria la actualización integral de dicho marco.

La presente orden deroga y sustituye a la Orden TES/369/2023, de 10 de abril, adaptando la política de seguridad del departamento a las mejores prácticas nacionales e internacionales en materia de ciberseguridad y protección de datos, e incorporando nuevos principios como el de mínimo privilegio, la clasificación de la información, la protección del soporte no electrónico y la vigilancia continua de los sistemas.

Asimismo, esta orden crea el Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones, ampliando su composición para incluir a los organismos públicos adscritos y reforzando su papel como órgano colegiado ministerial responsable de la coordinación, seguimiento y mejora continua de la seguridad de la información y de los servicios digitales del Ministerio.

Esta norma se dicta de conformidad con los principios de buena regulación previstos en el artículo 129 de la Ley 39/2015, de 1 de octubre –necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia y eficiencia–, constituyendo el instrumento más adecuado para garantizar la coherencia del sistema de gestión de la seguridad de la información del Ministerio y su alineación con el Esquema Nacional de Seguridad, el Reglamento General de Protección de Datos y la Ley Orgánica 3/2018, de 5 de diciembre, a fin de aplicar las medidas de seguridad al tratamiento de datos personales.

cve: BOE-A-2026-16757
Verificable en https://www.boe.es

En primer lugar, en virtud de los principios de necesidad y eficacia, esta iniciativa normativa está justificada por las razones expuestas, como instrumento más adecuado para dar cumplimiento al mandato contenido en el citado artículo 12.3 del Real Decreto 311/2022, de 3 de mayo. Además, se ajusta al principio de proporcionalidad, en tanto que la norma contiene la regulación imprescindible para atender sus objetivos. Se garantiza el principio de seguridad jurídica, en tanto que la norma es coherente con el resto del ordenamiento jurídico y, en particular, con el marco regulatorio en el ámbito de la política de seguridad de la información. Cumple con el principio de transparencia, ya que identifica claramente su propósito y, al tratarse de una norma organizativa su tramitación no ha requerido de la consulta pública previa ni de los trámites de audiencia e información pública. Finalmente, es también adecuada al principio de eficiencia, ya que no impone cargas administrativas.

En el proceso de su tramitación, ha sido informada favorablemente por los servicios jurídicos de la Abogacía del Estado en el departamento, por la Agencia Española de Protección de Datos y por la Comisión Ministerial de Administración Digital del Ministerio de Trabajo y Economía Social.

En su virtud, con la aprobación previa del Ministro para la Transformación Digital y de la Función Pública, dispongo:

Artículo 1. *Objeto.*

1. De acuerdo con lo previsto en el artículo 12.3 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, el objeto de esta orden ministerial es la aprobación de la política de seguridad de la información y de los servicios (en adelante política de seguridad o PSI), en el ámbito de la Administración Digital del Ministerio de Trabajo y Economía Social, así como la creación del Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones (en adelante, COSTIC) del Ministerio de Trabajo y Economía Social y la regulación de su composición, funcionamiento y funciones.

2. La PSI establece las orientaciones o directrices que rigen la actuación en el Ministerio de Trabajo y Economía Social, de las personas y entidades, en relación con la seguridad de los sistemas de información; entendiendo que un Sistema de Información es un conjunto organizado de recursos (físicos, lógicos, de comunicación, de datos, procedimientos, de servicios contratados y personas) que permite conseguir las especificaciones funcionales establecidas para el departamento.

Artículo 2. *Ámbito de aplicación.*

1. De acuerdo con lo previsto en los artículos 12.2, 12.3 y 13.1 del Real Decreto 311/2022, de 3 de mayo y el Real Decreto 502/2024, de 21 de mayo, por el que se desarrolla la estructura orgánica básica del Ministerio de Trabajo y Economía Social, y se modifica el Real Decreto 1052/2015, de 20 de noviembre, por el que se establece la estructura de las Consejerías de Empleo y Seguridad Social en el exterior y se regula su organización, funciones y provisión de puestos de trabajo, el ámbito subjetivo de esta PSI comprende todos los órganos del departamento y se aplicará, asimismo, a los organismos públicos y entidades de derecho público vinculados, dependientes o adscritos al mismo que no hayan aprobado formalmente su propia PSI.

2. La PSI es de obligado cumplimiento para todo el personal que desempeña sus funciones en el Ministerio de Trabajo y Economía Social, independientemente de su adscripción profesional (empleados públicos y apoyo técnico de empresas), que acceda a los sistemas de información y a la información del departamento, siendo aplicable a todos los sistemas de información y, en general, a toda la información que sea gestionada por el Departamento, con independencia de cuál sea su soporte, destino, adscripción o relación con el mismo.

cve: BOE-A-2026-16757
Verificable en https://www.boe.es

Artículo 3. *Marco normativo.*

1. El marco jurídico en el que se desarrollan las actividades del Ministerio de Trabajo y Economía Social en el ámbito de la prestación de los servicios electrónicos a la ciudadanía, sin perjuicio de la legislación específica, está integrado fundamentalmente por las normas contenidas en el anexo.

2. El Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Ministerio de Trabajo y Economía Social mantendrá actualizado dicho marco jurídico, especialmente las instrucciones técnicas de seguridad, de obligado cumplimiento, esenciales para lograr una adecuada, homogénea y coherente implantación de los requisitos y medidas recogidos en el Esquema Nacional de Seguridad.

Artículo 4. *Principios de la política de seguridad.*

Los principios básicos y requisitos de la seguridad de la información desarrollados bajo el marco de esta Política de Seguridad son los recogidos en el Esquema Nacional de Seguridad regulado por el Real Decreto 311/2022, de 3 de mayo, en particular, los previstos en sus capítulos II y III, y su normativa de desarrollo.

Artículo 5. *Estructura organizativa para la gestión de la seguridad.*

La estructura organizativa para la gestión de la seguridad de los sistemas de información del Ministerio de Trabajo y Economía Social y sus entes y organismos públicos adscritos, está compuesta por:

a) El COSTIC.
b) Los/as responsables de los sistemas de información.
c) Los/as responsables de la información.
d) Los/as responsables de los servicios.
e) Los/as responsables de la seguridad.
f) El/la Delegado o Delegada de Protección de Datos.
g) Los/as responsables del tratamiento de datos personales.
h) Los/as encargados o encargadas del tratamiento de datos personales.
i) Los/as responsables de la prestación de los servicios TIC.

Artículo 6. *El Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Ministerio de Trabajo y Economía Social.*

1. Se crea el COSTIC como órgano colegiado de carácter ministerial, adscrito a la Subsecretaría de Trabajo y Economía Social con la siguiente composición:

a) Presidencia: La persona titular de la Subsecretaría de Trabajo y Economía Social.
b) Vicepresidencia: La persona titular de la Jefatura del Gabinete Técnico de la Subsecretaría.
c) Vocalías:

1. Una persona representante designada por la persona titular de la Secretaría de Estado de Trabajo, con rango mínimo de subdirección general o asimilado.
2. Una persona representante designada por la persona titular de la Secretaría de Estado de Economía Social, con rango mínimo de subdirección general o asimilado.
3. Una persona representante designada por la persona titular de la Subsecretaría de Trabajo y Economía Social, con rango mínimo de subdirección general o asimilado.
4. La persona titular de la Subdirección General de Tecnologías de la Información y Comunicaciones, que, además, actuará como secretaría del COSTIC.
5. La persona responsable de la seguridad del Ministerio.
6. La persona responsable de la seguridad del Servicio Público de Empleo Estatal, O.A. (SEPE).

cve: BOE-A-2026-16757
Verificable en https://www.boe.es

7. La persona responsable de la seguridad del Fondo de Garantía Salarial, O.A. (FOGASA).

8. La persona responsable de la seguridad del Instituto Nacional de Seguridad y Salud en el Trabajo, O.A., M.P (INSST).

9. La persona responsable de la seguridad del Organismo Estatal de la Inspección de Trabajo y Seguridad Social (OEITSS).

10. La persona responsable de la seguridad del Consejo Económico y Social (CES).

2. La persona designada como Delegado o Delegada de Protección de Datos participará con voz, pero sin voto, en las reuniones del COSTIC, cuando en el mismo vayan a abordarse cuestiones relacionadas con el tratamiento de datos de carácter personal, así como siempre que se requiera su participación.

3. En casos de vacante, ausencia, enfermedad, abstención, recusación u otra causa legal, la persona a la que corresponda la Presidencia será sustituida por la persona titular de la Vicepresidencia. La persona que ostente la Secretaría del órgano será sustituida, en su caso, por el vocal designado por la persona titular de la Subsecretaría. En el caso de las vocalías, las personas que las desempeñen serán sustituidas por quienes designe el órgano que ha designado a las titulares.

4. Con carácter opcional, en función de los asuntos a tratar, otros miembros del Ministerio de Trabajo y Economía Social podrán incorporarse a las sesiones del COSTIC, con voz pero sin voto, incluyendo las personas responsables de la información, de los servicios, de los sistemas de información y grupos de trabajo especializados, ya sean de carácter interno, externo o mixto.

Artículo 7. *Funciones del Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Ministerio de Trabajo y Economía Social.*

Al COSTIC le corresponden las siguientes funciones:

a) Proponer, elaborar y aprobar las revisiones y actualizaciones de la política de seguridad, como normativa de seguridad de primer nivel, referenciada en el apartado a) del artículo 15 de esta norma.

b) Aprobar las revisiones y actualizaciones de la normativa de seguridad de segundo y cuarto nivel, propuestas y elaboradas por los/as responsables de los servicios y de la información, así como proponer, elaborar y aprobar las suyas propias, referenciadas en los apartados b) y d), respectivamente, del artículo 15 de esta norma.

c) Mantener actualizado el marco normativo aplicable a la seguridad de los sistemas de información.

d) Proponer planes de mejora de la seguridad de los sistemas de información, que podrán contemplar la aprobación, revisión y mejora de los planes estratégicos, los planes directores, los procedimientos, las normas y las líneas de actuación del departamento en materia de seguridad de los sistemas de información, con su dotación presupuestaria correspondiente, priorizando las actuaciones en materia de seguridad, cuando los recursos sean limitados.

e) Promover, aprobar, revisar y mejorar las políticas de auditoría, en especial del Esquema Nacional de Seguridad y de la protección de datos personales, de las unidades del departamento.

f) Realizar un seguimiento de los principales riesgos residuales e incidentes de seguridad y recomendar posibles actuaciones respecto a ellos.

g) Elaborar programas de formación destinados a formar y sensibilizar al personal en materia de seguridad de la información y, en particular, en materia de protección de datos de carácter personal.

h) Definir los mecanismos y resolver los conflictos entre las personas con roles de seguridad asignados.

cve: BOE-A-2026-16757
Verificable en https://www.boe.es

Artículo 8. *Organización y funcionamiento del Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Ministerio de Trabajo y Economía Social.*

1. El COSTIC se reunirá con carácter ordinario una vez al año y con carácter extraordinario cuando su presidente así lo convoque.

2. El COSTIC se podrá constituir, convocar, celebrar sus reuniones, adoptar acuerdos y remitir actas, tanto de forma presencial como a distancia, de conformidad con los artículos 17 y 18 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

3. La Secretaría del COSTIC levantará acta de las reuniones, siendo enviadas a la Presidencia de dicho comité para su aprobación, en su caso, en el pleno siguiente. Esta Secretaría realizará, junto con la persona responsable de la seguridad del departamento, todos los trabajos previos necesarios para las reuniones del COSTIC, apoyándose cuando lo requiera en las unidades, entidades y organismos del departamento.

Corresponde a la Secretaría del COSTIC la revisión de la política de seguridad, al menos anualmente, proponiendo mejoras de esta, así como las labores preparatorias para la actualización del marco normativo aplicable y la revisión de las normas de seguridad con la ayuda de las personas responsables de seguridad, presentándola para su toma en consideración por parte del COSTIC.

4. El COSTIC se regirá por esta orden y por las normas previstas para los órganos colegiados en la sección 3.ª del capítulo II del título preliminar de la Ley 40/2015, de 1 de octubre.

5. Para la válida constitución del COSTIC, a efectos de la celebración de sesiones, deliberaciones y toma de acuerdos, se requerirá la asistencia, presencial o a distancia, de la persona a la que corresponda la Presidencia y de la que ostente la Secretaría del órgano o, en su caso, de quienes les suplan, y la de la mitad, al menos, de sus miembros, de acuerdo con lo establecido en el apartado 2 del artículo 17 de la Ley 40/2015, de 1 de octubre.

Artículo 9. *La persona responsable del sistema.*

1. La persona responsable del sistema es quien tiene la responsabilidad de desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida.

2. Son funciones de la persona responsable del sistema:

a) Definir la tipología y sistema de gestión del sistema de información estableciendo los criterios de uso y los servicios disponibles en el mismo.

b) Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.

c) Proponer la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser adoptada por las personas responsables de la información afectada o del servicio afectado y la persona responsable de la seguridad.

d) Para las demás funciones que por su naturaleza así lo requieran, se coordinará con la Secretaría General Técnica; en particular, en lo relativo a las actuaciones de implementación, desarrollo y administración del Archivo Electrónico Único del departamento.

3. La persona titular de la Subdirección General de Tecnologías de la Información y Comunicaciones actuará como responsable del sistema en el ámbito del departamento. Cada uno de los entes y organismos públicos adscritos al ministerio, a los que sea de aplicación esta política de seguridad, designarán una persona o unidad responsable del sistema.

cve: BOE-A-2026-16757
Verificable en https://www.boe.es

Artículo 10. *Las personas o unidades administrativas responsables de la información.*

1. Conforme a los artículos 13 y 41 del Real Decreto 311/2022, de 3 de mayo, es responsable de la información la persona o unidad administrativa que tiene la potestad de establecer los requisitos de la información tratada y su implicación en la valoración del sistema de información del que forme parte.

2. Serán funciones de la persona responsable de la información, dentro de su ámbito de actuación, las siguientes:

a) Establecer los requisitos de la información tratada.

b) Valorar el impacto que tendría un incidente que afectase a la seguridad de la información con perjuicio para la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad.

c) La valoración de las consecuencias de un impacto negativo sobre la seguridad de la información se efectuará atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio y el respeto de la legalidad y de los derechos de los ciudadanos.

d) Aceptar los riesgos residuales respecto de la información, calculados en el análisis de riesgos.

e) Adoptar, de acuerdo con las personas responsables del servicio afectado y de seguridad, la decisión de la suspensión del manejo de una cierta información a propuesta de la persona responsable del sistema cuando haya sigo informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos.

f) Proponer y elaborar las revisiones y actualizaciones de la normativa de seguridad de segundo nivel, que afectasen a la información de su competencia, referenciadas en el apartado b) del artículo 15 de esta norma.

g) Proponer y elaborar la documentación de la normativa de seguridad de cuarto nivel, que afectasen a la información de su competencia, referenciadas en el apartado d) del artículo 15 de esta norma.

3. La designación de la persona responsable de la información corresponderá a la persona titular de cada órgano superior y de cada órgano directivo dependiente del ministerio, conforme a su ámbito competencial y a su organización interna. En el caso de los entes y organismos públicos adscritos al ministerio, dicha designación corresponderá a la persona titular del órgano directivo que, de acuerdo con su norma de creación y su estructura organizativa, tenga atribuida la competencia para efectuarla.

Artículo 11. *Las personas o unidades administrativas responsables de los servicios.*

1. Conforme a los artículos 13 y 41 del Real Decreto 311/2022, de 3 de mayo, es responsable del servicio la persona o unidad administrativa, que tiene la potestad de establecer los requisitos del servicio prestado y su implicación en la valoración del nivel de seguridad de dicho servicio.

2. Serán funciones de la persona responsable del servicio, dentro de su ámbito de actuación las siguientes:

a) Determinar los requisitos de los servicios prestados.

b) Valorar el impacto que tendría un incidente que afectase a la seguridad de los servicios con perjuicio para la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad.

c) La valoración de las consecuencias de un impacto negativo sobre la seguridad de los servicios se efectuará atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los ciudadanos.

cve: BOE-A-2026-16757
Verificable en https://www.boe.es

d) Aceptar los riesgos residuales respecto de los servicios, calculados en el análisis de riesgos.

e) Adoptar, de acuerdo con las personas responsables de la información y de seguridad, la decisión de la suspensión de la prestación de un cierto servicio a propuesta de la persona responsable del sistema cuando haya sigo informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos.

f) Proponer y elaborar las revisiones y actualizaciones de la normativa de seguridad de segundo nivel, que afectasen al servicio de su competencia, referenciadas en el apartado b) del artículo 15 de esta norma.

g) Proponer y elaborar la documentación de la normativa de seguridad de cuarto nivel, que afectasen al servicio de su competencia, referenciadas en el apartado d) del artículo 15 de esta norma.

3. La designación de la persona responsable de los servicios corresponderá a la persona titular de cada órgano superior y de cada órgano directivo dependiente del ministerio, conforme a su ámbito competencial y a su organización interna. En el caso de los entes y organismos públicos adscritos, dicha designación corresponderá a la persona titular del órgano superior o directivo que, de acuerdo con su norma de creación y su estructura organizativa, tenga atribuida la competencia para efectuarla.

4. La persona responsable de la información y la responsable del servicio podrán coincidir en una misma persona o unidad administrativa.

Artículo 12. *La persona responsable de la seguridad.*

1. Conforme al artículo 13 del Real Decreto 311/2022, de 3 de mayo, la persona responsable de seguridad es la persona que determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, y supervisa la implantación de las medidas necesarias para garantizar que se satisfacen dichos requisitos y reportar sobre estas cuestiones.

2. Serán funciones de la persona responsable de seguridad, dentro de su ámbito de actuación, las siguientes:

a) Mantener y verificar el nivel adecuado de seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información.

b) Promover la formación y concienciación en materia de seguridad de la información.

c) Determinar la categoría de seguridad del sistema en colaboración con la persona responsable del sistema y con las responsables de la información y del servicio.

d) Participar en la elaboración e implantación de los planes de mejora de la seguridad y, en su caso, en la de los planes de continuidad, procediendo a su validación.

e) Gestionar y asegurar las revisiones externas o internas del sistema, incluyendo auditorías que serán transmitidas a las personas responsables de los sistemas de información para el seguimiento y resolución de las deficiencias encontradas.

f) Gestionar los procesos de certificación y las declaraciones de aplicabilidad pertinentes de los sistemas de información.

g) Generar y mantener actualizada la documentación relativa a su ámbito de responsabilidad.

h) Proponer, elaborar y aprobar la documentación de la normativa de seguridad de tercer nivel, referenciadas en el apartado c) del artículo 15 de esta norma.

i) Adoptar, de acuerdo con las personas responsables de la información y del servicio afectado, la decisión de la suspensión del manejo de una cierta información o la prestación de un cierto servicio a propuesta de la persona responsable del sistema cuando haya sido informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos.

j) Aprobar las declaraciones de aplicabilidad y conformidad con el Esquema Nacional de Seguridad.

cve: BOE-A-2026-16757
Verificable en https://www.boe.es

3. La persona titular de la Subsecretaría designará a la persona responsable de seguridad del ministerio. Asimismo, designará al responsable de seguridad de cada ente y organismo público adscrito al departamento, a propuesta del organismo correspondiente.

De acuerdo con lo previsto en el artículo 13.3 del Real Decreto 311/2022, de 3 de mayo, la persona responsable de la seguridad será distinta de la responsable del sistema, no debiendo existir dependencia jerárquica entre ambas. En aquellas situaciones excepcionales en las que la ausencia justificada de recursos haga necesario que ambas funciones recaigan en la misma persona o en distintas personas entre las que exista relación jerárquica, deberán aplicarse medidas compensatorias para garantizar la finalidad del principio de diferenciación de responsabilidades previsto en el artículo 11 del citado real decreto.

Cuando la complejidad, distribución, separación física de sus elementos o número de usuarios de los sistemas de información lo justifiquen, la persona titular de la Subsecretaría podrá designar a las personas responsables de seguridad delegadas que considere necesarias, que tendrán dependencia funcional directa de la persona responsable de seguridad del ministerio y que serán responsables, en su ámbito, de todas aquellas acciones que aquella les delegue.

Para garantizar que la persona responsable de seguridad no reciba instrucciones que limiten el desempeño de sus funciones, las desempeñará con independencia de las unidades que gestionen las tecnologías de la información y comunicaciones y, en estas funciones dependerá de la Presidencia del COSTIC.

Artículo 13. *Delegado o delegada de protección de datos.*

1. El delegado o delegada de protección de datos tiene carácter asesor y supervisor para el cumplimiento de lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, en adelante Reglamento General de Protección de Datos, y demás normativa aplicable sobre protección de datos personales, debiéndose garantizar su independencia dentro de la organización y evitar cualquier conflicto de intereses, así como proveer de los medios necesarios para el desarrollo de sus funciones conforme al artículo 39 del mencionado Reglamento. El delegado o delegada de protección de datos será designado/a atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39 del mencionado Reglamento.

2. El asesoramiento y supervisión del delegado o delegada de protección de datos se extiende a aquellas medidas de seguridad que se quieran implementar con finalidades distintas a garantizar la protección de datos, en la medida que impliquen un tratamiento adicional de datos personales.

Artículo 14. *Tratamiento de datos personales.*

1. Se aplicarán a los datos de carácter personal que sean objeto de tratamiento por parte del Ministerio de Trabajo y Economía Social las medidas de seguridad apropiadas derivadas del análisis de riesgos de privacidad, así como de la evaluación de impacto relativa a la protección de datos, tal y como se detalla en el artículo 32 del Reglamento General de Protección de Datos.

Cuando un sistema de información trate datos personales, la persona responsable o la persona encargada del tratamiento, asesoradas por la persona designada como delegada de protección de datos, realizarán un análisis de riesgos, conforme al artículo 24 del Reglamento General de Protección de Datos.

cve: BOE-A-2026-16757
Verificable en https://www.boe.es

La identificación de los riesgos específicos para los derechos y libertades de las personas físicas en relación con los tratamientos efectuados por la entidad debe ser previo al análisis de riesgos de sistemas donde se implementen los tratamientos, con el fin de permitir que el sistema de seguridad sea adecuado al riesgo que los tratamientos suponen para los derechos y libertades de las personas.

Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, la persona responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales, de conformidad con lo establecido en el artículo 35 del Reglamento General de Protección de Datos.

Además, en cumplimiento de la disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre, se aplicarán las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento General de Protección de Datos.

En el caso de que el análisis de riesgos y la evaluación de impacto en su caso, determine medidas agravadas respecto a la normativa recogida en el anexo II del Real Decreto 311/2022, de 3 de mayo, dichas medidas serán las que se implementarán en la protección de datos personales.

2. En función de las diversas situaciones que puedan producirse en materia de protección de datos personales, se establecerá la oportuna coordinación con la persona designada como delegada de protección de datos, de conformidad con el artículo 37 del Reglamento General de Protección de Datos y el artículo 34 de la Ley Orgánica 3/2018, de 5 de diciembre, y en la medida en que sea preciso, con las personas responsables y con las personas encargadas del tratamiento de datos personales.

Especialmente, se prestará apoyo a la persona designada como delegada de protección de datos, para la elaboración de propuestas o informes relativos a las reclamaciones de los interesados y respuestas a los requerimientos de la Agencia Española de Protección de Datos.

Artículo 15. *Normativa de seguridad.*

La normativa de seguridad del Ministerio de Trabajo y Economía Social se estructura en cuatro niveles siendo de obligada aplicación los tres primeros de la siguiente manera:

a) Primer nivel: La política de seguridad que queda regulada en esta orden ministerial.

b) Segundo nivel: Las normas de seguridad, instrucciones, protocolos, entre otros instrumentos, que concretan la política de seguridad y que deben especificar de forma concisa, transparente, inteligible y accesible, con un lenguaje claro y sencillo los objetivos de seguridad que se desean alcanzar.

c) Tercer nivel: Los procedimientos de seguridad, que se describen en los instrumentos referidos en el apartado anterior, indican explícitamente y paso a paso cómo realizar una cierta actividad. Cada procedimiento debe detallar:

1.º En qué condiciones debe aplicarse.
2.º Quiénes son los que deben llevarlo a cabo.
3.º Qué es lo que hay que hacer en cada momento, incluyendo, en su caso, el registro de la actividad realizada.
4.º Cómo se miden sus resultados.
5.º Cómo se reportan posibles mejoras y deficiencias en los procedimientos.

cve: BOE-A-2026-16757
Verificable en https://www.boe.es

d) Cuarto nivel: Abarca la documentación de buenas prácticas, las recomendaciones formuladas y cualesquiera otros contenidos que afecten de manera no esencial a los conceptos constitutivos de los niveles anteriores.

A toda la documentación generada por parte del Ministerio de Trabajo y Economía Social relativa a su Sistema de Gestión de la Seguridad de la Información le serán de aplicación los procedimientos internos de gestión documental.

Artículo 16. *Actuación y efectos respecto a la información correspondiente a otros entes o servicios de competencia ajena al departamento.*

1. Cuando el Ministerio de Trabajo y Economía Social preste servicios a otros organismos o maneje información de otros organismos, se hará partícipes a los mismos de la política de seguridad. El Ministerio de Trabajo y Economía Social definirá y aprobará los canales para la coordinación de la información y los procedimientos de actuación para la reacción ante incidentes de seguridad, así como el resto de las actuaciones que el departamento lleve a cabo en materia de seguridad en relación con otros organismos.
2. Cuando el Ministerio de Trabajo y Economía Social utilice servicios proporcionados por terceros o ceda información a terceros, se les hará partícipe de la política de seguridad y de la normativa de seguridad existente que atañe a dichos servicios o información. Estos sujetos que se relacionen con el ministerio quedarán vinculados por las obligaciones establecidas en la mencionada normativa y podrán desarrollar sus propios procedimientos operativos para ejecutarlas. Se establecerán procedimientos específicos de comunicación y resolución de incidencias y se garantizará que su personal esté adecuadamente concienciado y formado en materia de seguridad.
3. Cuando algún aspecto de la política de seguridad no pueda ser satisfecho por una tercera parte según lo dispuesto en los apartados anteriores, se requerirá un informe de la persona responsable de seguridad del departamento u organismo adscrito al mismo, que precise los riesgos en los que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por las personas responsables de la información y de los servicios afectados antes de que la prestación de servicios o la cesión de la información continúen su ejecución.
4. Cuando la información contenga datos de carácter personal quedará sujeta a la normativa sobre protección de datos personales por la que están obligados a velar tanto las personas responsables como las encargadas del tratamiento.

Artículo 17. *Formación y concienciación.*

1. Todo el personal del Ministerio de Trabajo y Economía Social relacionado con la información, los servicios y los sistemas de información deberá conocer sus deberes y obligaciones en esta materia de seguridad de la información e identificar de forma inequívoca a las personas responsables de velar por su cumplimiento.
2. Para garantizar la seguridad de las tecnologías de la información aplicable a los sistemas y servicios del Ministerio de Trabajo y Economía Social, el COSTIC propondrá los mecanismos necesarios para desarrollar las actividades para la concienciación y la formación específica necesaria e imprescindible, en materia de política de seguridad de la información, en todos los niveles de la organización.

Disposición adicional primera. *Política de seguridad de la información de los organismos públicos y entidades de derecho público vinculados, dependientes o adscritos al Ministerio de Trabajo y Economía Social.*

1. De acuerdo con lo previsto en el artículo 12.3 del Real Decreto 311/2022, de 3 de mayo, y el artículo 2 de esta orden, los organismos y entidades vinculados, dependientes o adscritos al Ministerio de Trabajo y Economía Social podrán contar con su propia

cve: BOE-A-2026-16757
Verificable en https://www.boe.es

política de seguridad, aprobada mediante resolución del órgano competente, que será coherente con la del Departamento aprobada por esta orden.

2. En caso de discrepancia, prevalecerá la política de seguridad de la información definida en esta orden ministerial.

3. En todo caso, los organismos y entidades vinculados, dependientes o adscritos al Departamento deberán informar de forma inmediata a la Subdirección General de Tecnologías de la Información y Comunicaciones sobre cualquier incidencia o riesgo que pueda poner en peligro la seguridad de los sistemas informáticos de este.

Disposición adicional segunda. *No incremento del gasto público.*

Las medidas incluidas en esta orden no supondrán incremento del gasto, y serán atendidas con los medios personales, técnicos y presupuestarios asignados al Ministerio de Trabajo y Economía Social.

Disposición derogatoria única. *Derogación normativa.*

Queda derogada la Orden TES/369/2023, de 10 de abril, por la que se aprueba la política de seguridad de la información y de los servicios en el ámbito de la administración digital del Ministerio de Trabajo y Economía Social y se crea el Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del departamento.

Disposición final primera. *Instrucciones de aplicación.*

La persona titular de la Subsecretaría de Trabajo y Economía Social podrá dictar las instrucciones necesarias para el adecuado cumplimiento de esta orden.

Disposición final segunda. *Entrada en vigor.*

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

Madrid, 23 de julio de 2026.–La Vicepresidenta Segunda del Gobierno y Ministra de Trabajo y Economía Social, Yolanda Díaz Pérez.

ANEXO

El marco jurídico en que se desarrollan las actividades del Ministerio de Trabajo y Economía Social en el ámbito de la prestación de los servicios electrónicos a la ciudadanía, sin perjuicio de la legislación específica, está integrado fundamentalmente por las siguientes normas, así como sus posibles actualizaciones:

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

b) Directiva (UE) 2022/2555 del Parlamento europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión.

c) Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

d) La Ley 9/1968, de 5 de abril, sobre secretos oficiales.

e) Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

f) Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

g) Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

cve: BOE-A-2026-16757
Verificable en https://www.boe.es

h) Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.

i) Reglamento de actuación y funcionamiento del sector público por medios electrónicos, aprobado por Real Decreto 203/2021, de 30 de marzo.

j) Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, y las Instrucciones Técnicas de Seguridad para su aplicación aprobadas por la persona titular del Ministerio para la Transformación Digital y de la Función Pública, de acuerdo con lo previsto en la disposición adicional segunda de dicho real decreto.

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

l) Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en al ámbito de la Administración Electrónica.

m) 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.

n) Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional el 12 de abril de 2019, publicada por Orden PCI/487/2019, de 26 de abril.

cve: BOE-A-2026-16757
Verificable en https://www.boe.es