III. OTRAS DISPOSICIONES

MINISTERIO DE JUVENTUD E INFANCIA

1905 *Orden JUI/29/2026, de 14 de enero, por la que se aprueba la Política de Seguridad de la Información en el ámbito de la administración electrónica del Ministerio de Juventud e Infancia.*

El marco de relación entre la Administración Pública y los ciudadanos a través de los medios electrónicos se encuentra establecido en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. En su artículo 13 se recoge, entre los derechos de las personas en sus relaciones con las Administraciones Públicas, el relativo «a la protección de datos de carácter personal, y en particular a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas».

Por otra parte, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en su artículo 3, trata los principios generales relativos a las relaciones de las Administraciones Públicas a través de medios electrónicos. Así mismo, en su artículo 156 se contempla el Esquema Nacional de Interoperabilidad y el Esquema Nacional de Seguridad (en adelante, ENS). Ambas leyes han sido objeto de desarrollo en estas materias a través del Reglamento de actuación y funcionamiento del sector público por medios electrónicos, aprobado por Real Decreto 203/2021, de 30 de marzo.

Asimismo, el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante ENS), tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de las relaciones entre la Administración Pública y los ciudadanos a través de los medios electrónicos, estableciendo los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada y los servicios prestados.

Así, el artículo 12.3 del citado Real Decreto 311/2022, de 3 de mayo, exige que, en la Administración General del Estado, todos los ministerios dispongan formalmente de su política de seguridad que se aprobará por la persona titular del Departamento. Esta política de seguridad se establecerá con base en los principios básicos recogidos en el capítulo II de la propia norma: seguridad como proceso integral, gestión de la seguridad basada en los riesgos, prevención, detección, respuesta y conservación, existencia de líneas de defensa, vigilancia continua, reevaluación periódica y diferenciación de responsabilidades. Adicionalmente, el artículo 12.6 establece que las mencionadas políticas desarrollarán una serie de requisitos mínimos.

Del mismo modo, la política de seguridad de la Información debe adecuarse y ser coherente con lo establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, así como con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

En atención a cuanto ha quedado expuesto, el Ministerio de Juventud e Infancia ha situado los sistemas de Tecnologías de la Información y de las Comunicaciones (TIC) como elementos estratégicos para el desarrollo y cumplimiento de las competencias que se le atribuyen. Dichos sistemas deben ser administrados tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la confidencialidad de la información tratada, la integridad, la disponibilidad, la autenticidad, o la trazabilidad de los servicios prestados.

En un entorno de amenazas digitales en constante evolución y de distinta naturaleza, y a tenor de una sociedad con gran exposición digital, la gestión de la seguridad se convierte en una necesidad para las Administraciones Públicas en general, y este

cve: BOE-A-2026-1905
Verificable en https://www.boe.es

Departamento en particular, a fin de asegurar el ejercicio de las funciones encomendadas. Siendo imprescindible la implementación de un plan de seguridad que vele por la calidad de los servicios, y la información en sí misma. Un Plan que permita gestionar los riesgos relacionados con las TIC y confiera una estructura organizativa y operativa para poder implantar las medidas requeridas.

Con la presente orden se pretende, por tanto, aprobar la Política de Seguridad de la Información del Ministerio de Juventud e Infancia, así como establecer la estructura organizativa para definirla, implantarla y gestionarla.

Esta norma está en consonancia con los principios de buena regulación recogidos en el artículo 129 de la Ley 39/2015, de 1 de octubre, de necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia, y eficiencia.

La norma es respetuosa con el principio de necesidad de aprobar la Política de Seguridad de la Información en el ámbito la de Administración Digital del Ministerio de Juventud e Infancia, de acuerdo con la nueva estructura organizativa de la Administración General del Estado, y da cumplimiento al mandato contenido en el Real Decreto 311/2022, de 3 de mayo.

Adicionalmente, establece una regulación coherente con el resto del ordenamiento jurídico, es predecible y clara y contribuye a dotar de mayor seguridad jurídica a la organización y funcionamiento de la Administración General del Estado, en lo que se refiere al plan de seguridad del Departamento.

Se da cumplimiento también con el principio de transparencia, ya que identifica claramente su propósito y la memoria de análisis de impacto normativo que la acompaña, accesible a la ciudadanía, ofrece una explicación completa de su contenido. Además, es precisamente la publicación de esta norma la que permite dar a conocer a la ciudadanía la creación y existencia de la política de Seguridad de este Departamento.

Finalmente, es también adecuada al principio de eficiencia, ya que, con su regulación y rango normativo, cumple con dicho principio, puesto que es el medio más adecuado y sencillo para cumplir los objetivos propuestos, y no impone cargas administrativas.

Durante su tramitación, se han recabado los informes de la Comisión Ministerial de Administración Digital del Ministerio de Juventud e Infancia, de la Secretaría General Técnica y de la persona designada Delegada de Protección de Datos del Departamento, así como de la Agencia Española de Protección de Datos.

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

Artículo 1. *Objeto y ámbito de aplicación.*

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 en al ámbito de la Administración Electrónica, constituye el objeto de la presente orden la aprobación de la Política de Seguridad de la Información (en adelante, PSI) en el ámbito de la Administración Digital del Ministerio de Juventud e Infancia, así como del marco organizativo global en materia de Seguridad de la Información del Departamento.

2. La PSI será de obligado cumplimiento para todos los órganos del Departamento, así como para los organismos públicos y entidades vinculados o dependientes del mismo que no tengan establecida su propia política de seguridad.

3. La PSI será de obligado cumplimiento para todo el personal, propio o ajeno, en el uso de medios digitales y en lo relativo a la información en soporte papel que gestionen en el ámbito de sus competencias. Será también de aplicación a toda persona que acceda tanto a los Sistemas TIC como a la propia información que sea gestionada por el Departamento, con independencia de cuál sea su destino, adscripción o relación con este.

cve: BOE-A-2026-1905
Verificable en https://www.boe.es

Artículo 2. *Misión del Departamento.*

El Ministerio de Juventud e Infancia, de acuerdo con el Real Decreto 211/2024, de 27 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio de Juventud e Infancia, es el Departamento de la Administración General del Estado al que corresponde la propuesta y ejecución de la política del Gobierno en materia de juventud y de protección de las personas menores de edad.

Artículo 3. *Marco normativo.*

1. El marco normativo en que se desarrollan las actividades del Ministerio de Juventud e Infancia en el ámbito de la prestación de los servicios electrónicos a los ciudadanos, sin perjuicio de la legislación específica, se compone, fundamentalmente, de las siguientes normas:

a) El Texto refundido de la Ley de Propiedad Intelectual, aprobado por Real Decreto Legislativo 1/1996, de 12 de abril, y su normativa de desarrollo.
b) El Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.
c) El 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.
d) La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
e) La Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
f) El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
g) La Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.
h) El Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información que traspone la Directiva Europea NIS (Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016.
i) La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
j) La Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional.
k) 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.
l) El Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.
m) El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en al ámbito de la Administración Electrónica y las Instrucciones Técnicas de Seguridad para su aplicación dictadas por la persona titular de la Secretaría de Estado de Función Pública, de acuerdo con lo previsto en la disposición adicional segunda de dicho real decreto.
n) El Real Decreto 829/2023, de 20 de noviembre, por el que se reestructuran los departamentos ministeriales.
o) El Real Decreto 211/2024, de 27 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio de Juventud e Infancia.
p) La Orden JUI/844/2024, de 31 de julio, por la que se crea la Comisión Ministerial de Administración Digital del Ministerio de Juventud e Infancia y se regula su composición y funciones.

cve: BOE-A-2026-1905
Verificable en https://www.boe.es

q) Orden JUI/833/2024, de 30 de julio, por la que se crea y regula el Portal de Internet del Ministerio de Juventud e Infancia.

r) Orden JUI/893/2024, de 20 de agosto, por la que se crea la sede electrónica asociada del Ministerio de Juventud e Infancia.

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

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

2. Del mismo modo, las actuaciones que desarrolle el Ministerio de Juventud e Infancia en aplicación de la presente orden se adecuarán a las normas aplicables a la Administración Electrónica del Departamento que desarrollen o complementen las disposiciones normativas citadas en el apartado anterior vinculadas al ámbito de aplicación de la PSI.

Artículo 4. *Principios de la Política de Seguridad de la Información.*

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. *Normativa interna de seguridad.*

1. El desarrollo normativo sobre seguridad de la información es de obligado cumplimiento y se estructura de manera que cada norma de un determinado nivel de desarrollo se fundamente en las normas de nivel superior. Dichos niveles de desarrollo normativo son los siguientes:

a) Primer nivel: constituido por la PSI que se aprueba mediante la presente orden.

b) Segundo nivel: constituido por las normas y directrices generales de seguridad que, respetando lo estipulado por la PSI, determinan el ámbito de uso de los recursos tecnológicos del Departamento y, en su caso, de sus organismos públicos y entidades dependientes desde el punto de vista de la seguridad, sin considerar aspectos técnicos relativos a su implementación.

Este segundo nivel normativo deberá limitarse única y exclusivamente al ámbito específico de las competencias del Departamento o de los organismos adscritos a la presente PSI. Este ámbito vendrá determinado por los sistemas de información y servicios TIC que sean prestados y gestionados directamente por este Departamento o los organismos adscritos a la presente PSI. En otro caso, se entienden de obligado conocimiento y cumplimiento por parte de toda persona que acceda a dichos servicios la PSI del Departamento competente, así como los desarrollos normativos de segundo nivel correspondientes a dichos servicios TIC no prestados o gestionados directamente por el ministerio de Juventud e Infancia, o los organismos adscritos a la presente PSI.

Las normas y directrices generales de seguridad de este segundo nivel normativo serán aprobadas por resolución de la persona titular de la Subsecretaría de Juventud e Infancia, a propuesta del Comité de Seguridad de la Información del Departamento.

c) Tercer nivel: constituido por los procedimientos operativos de seguridad, guías, e instrucciones técnicas que sean adoptados cumpliendo con lo expuesto en los niveles normativos anteriores, y que determinan las acciones, tareas o instrucciones de carácter técnico a realizar en el desempeño de un proceso aplicado a ámbitos o sistemas de información particulares.

Este tercer nivel normativo deberá limitarse única y exclusivamente al ámbito específico de las competencias del Departamento o de los organismos adscritos a la presente PSI. Este ámbito vendrá determinado por los sistemas de información y servicios de tecnologías de la información y de las comunicaciones que sean prestados y gestionados directamente por este Departamento o los organismos adscritos a la

cve: BOE-A-2026-1905
Verificable en https://www.boe.es

presente PSI. En otro caso, se entienden de obligado conocimiento y cumplimiento por parte de toda persona que acceda a dichos servicios la PSI del Departamento competente, así como los desarrollos normativos de tercer nivel correspondientes a dichos servicios TIC no prestados o gestionados directamente por el ministerio de Juventud e Infancia, o los organismos adscritos a la presente PSI.

Su aprobación corresponde a la persona Responsable de la Seguridad, previo acuerdo en el Comité de Seguridad de la Información del Departamento.

2. La normativa interna de seguridad podrá incorporar asimismo otros instrumentos tales como estándares de seguridad, buenas prácticas, informes técnicos, a criterio de cada uno de los órganos, organismos y entidades comprendidos en el ámbito subjetivo de la presente PSI y siempre dentro del ámbito de sus competencias y responsabilidades.

3. El personal de cada uno de los órganos, organismos y entidades comprendidos en el ámbito subjetivo de la presente PSI tendrá la obligación de conocer y cumplir, además de la presente PSI, todas las directrices generales, normas y procedimientos de seguridad de la información que puedan afectar a sus funciones.

4. Este marco normativo estará a disposición de todo el personal de los órganos, organismos y entidades comprendidos en el ámbito subjetivo de la presente PSI a través de una sección diferenciada en la intranet del Departamento y, en su caso, de las intranets de los mencionados organismos y entidades.

Artículo 6. *Estructura organizativa.*

1. La organización de la seguridad debe tener en cuenta la propia organización del Departamento, en consecuencia, las responsabilidades en seguridad de la información deben emerger de todos los órganos del ministerio, garantizándose la actuación coordinada y eficaz, de acuerdo con lo previsto en el artículo 11 del Real Decreto 311/2022, de 3 de mayo, y en la correspondiente guía CCN-STIC sobre responsabilidades y funciones en el ENS.

2. La estructura organizativa para la gestión de la seguridad de la información en el ámbito descrito por la PSI del Ministerio de Juventud e Infancia está compuesta por los siguientes agentes:

a) La persona titular de la Subsecretaría de Juventud e Infancia.
b) El Comité de Seguridad de la Información del Departamento.
c) La persona designada como Responsable de la Seguridad.
d) La persona designada como Responsable del Sistema.
e) Las personas designadas como Responsables de la Información y Responsables del Servicio.
f) Las personas designadas como Delegadas de Protección de Datos del Departamento y, en su caso, de los distintos organismos públicos dependientes.

Artículo 7. *Competencias de la persona titular de la Subsecretaria de Juventud e Infancia en el ámbito de la Seguridad de la Información.*

La persona titular de la Subsecretaría de Juventud e Infancia es, en el ejercicio de sus competencias, la responsable última del funcionamiento de los servicios. En particular:

a) Coordinará todas las actividades relacionadas con la seguridad de los servicios prestados por la Subsecretaría, tanto de carácter horizontal, común o compartido, como de carácter sectorial.
b) Impulsará la adecuación a la normativa aplicable de seguridad de la información y de protección de datos.
c) Será responsable de la modificación y actualización de esta PSI, así como de aprobar la normativa de seguridad de segundo nivel propuesta por el Comité de Seguridad de la Información del Departamento.

cve: BOE-A-2026-1905
Verificable en https://www.boe.es

d) Será responsable de promover la mejora continua en la gestión de la seguridad de la información en el ámbito del Departamento.

Artículo 8. *El Comité de Seguridad de la Información del Departamento.*

1. Con carácter permanente, se crea el Comité de Seguridad de la Información del Ministerio de Juventud e Infancia (en adelante, CSID) con el objeto de dotar al Departamento de un órgano colegiado de carácter horizontal responsable de establecer, gestionar, coordinar y supervisar la estrategia en materia de seguridad de la información, y el cumplimiento del Real Decreto 311/2022, de 3 de mayo.

2. El CSID estará compuesto por las siguientes personas:

a) Presidencia: Corresponderá a la persona titular de la División de Tecnologías y Servicios de la Información (en adelante DTSI). Tendrá voz y voto de calidad en la toma de decisiones del CSID. Podrá autorizar la asistencia a las reuniones de expertos en las materias que se vayan a tratar, ya sean personal interno o externo, que tendrán el carácter de asesores, con voz, pero sin voto.

b) Vocalías:

1.º La persona designada como Responsable del Sistema.

2.º Las personas designadas como Responsables de la Información, y como Responsables del Servicio en el ámbito del Departamento.

3.º Las personas designadas como Delegada de Protección de Datos del Ministerio, y, en su caso, como Delegada de Protección de Datos de los organismos públicos y entidades adscritos al departamento. Actuarán, con voz, pero sin voto para garantizar su independencia en atención a la naturaleza de sus funciones de apoyo y asistencia. No obstante, lo anterior, se recogerá en el acta el parecer de la personas designadas Delegadas de Protección de Datos si no coinciden con la decisión adoptada por el Comité de Seguridad de la Información del Departamento.

c) Secretaría: Corresponderá a la persona designada como Responsable de la Seguridad del Departamento, que tendrá voz y voto y que ejecutará las decisiones del CSID, convocará sus reuniones y preparará los temas a tratar.

3. La persona titular de la Presidencia podrá autorizar la asistencia, en razón de los asuntos a tratar, a representantes de cualquier órgano y unidad que accedan a sistemas de información del Departamento, así como a personal experto en calidad de asesores, que actuarán con voz, pero sin voto.

4. En casos de vacante, ausencia, enfermedad, abstención, recusación u otra causa legal, el Presidente será sustituido por aquel que designe la persona titular de la Subsecretaría de Juventud e Infancia, y en su defecto, por la persona del órgano colegiado de mayor jerarquía, antigüedad y edad, por este orden. En el caso de las Vocalías, estas serán sustituidas por aquellos representantes que estos designen.

5. El CSID se reunirá con carácter ordinario, como mínimo, dos veces al año o con carácter extraordinario cuando la Presidencia lo considere necesario si:

a) Surgieran incidencias de seguridad graves.

b) Fuera necesario establecer nuevas directrices de seguridad.

c) Existiera una solicitud motivada de la persona designada Responsable de la Seguridad.

6. Son funciones del CSID:

a) Elaborar estudios, análisis y propuestas de modificación y actualización de la Política de Seguridad, de la estrategia de evolución del Departamento en el ámbito de la seguridad y de la normativa de seguridad de la información de segundo nivel.

cve: BOE-A-2026-1905
Verificable en https://www.boe.es

b) Velar por la coherencia y armonización de la normativa y actuaciones en materia de seguridad de la información entre los distintos servicios ofrecidos por los órganos del Departamento, ya sean los de carácter común, horizontal o sectorial.

c) Estudiar y proponer actividades de concienciación y formación en materia de seguridad, velar e impulsar el cumplimiento del cuerpo normativo a que se refiere el artículo 4, e impulsar y promover la formación y concienciación en materia de seguridad de la información.

d) Realizar cualquier otra actividad de asesoría, formulación de recomendaciones, o propuesta de iniciativas, en materia de seguridad.

e) Tomar aquellas decisiones que garanticen la seguridad de la información y de los servicios del Departamento, así como la evaluación y seguimiento de las decisiones tomadas para satisfacer los requisitos de seguridad de la información y de los servicios.

f) Informar periódicamente a la persona titular de la Subsecretaría de Juventud e Infancia sobre el estado de la seguridad en el ámbito de esta Política de Seguridad. Para ello podrá utilizar informes de incidentes de seguridad, resultados de auditorías y análisis de riesgos realizados, y, en general, cualquier información de seguridad relevante que pueda recabar en el desarrollo de sus funciones.

g) Cualquier otra función en el ámbito de la seguridad de la información y los servicios que le sea encomendada a través de la normativa de seguridad de segundo nivel al respecto.

7. En el establecimiento de los acuerdos y toma de decisiones serán adoptados por mayoría de votos de los miembros del CSID.

8. El CSID se regirá por las normas de funcionamiento previstas en la presente orden y, en lo no contemplado en ellas, por las normas previstas para los órganos colegiados en la sección 3.ª del capítulo II del título preliminar de la Ley 40/2015, de 1 de octubre.

Artículo 9. *La persona designada Responsable de la Seguridad.*

1. La persona designada Responsable de la Seguridad (de los sistemas de información), será nombrada por la persona titular de la DTSI y, de acuerdo con lo previsto en el artículo 13 del Real Decreto 311/2022, de 3 de mayo, y en la correspondiente guía CCN-STIC sobre roles y funciones en el ENS.

2. El ámbito de actuación de la persona designada Responsable de la Seguridad se extiende a todos los servicios de tecnologías de la información y las comunicaciones prestados y/o gestionados por el Departamento, debiendo velar por la coherencia y armonización de las normas, procedimientos y actuaciones en los diferentes ámbitos.

3. Le corresponde el desempeño de las siguientes funciones:

a) Elaborar la normativa de seguridad de segundo nivel, definida en el artículo 4, así como aprobar los procedimientos, guías, e instrucciones técnicas vinculadas al tercer nivel normativo, previo acuerdo en el CSID.

b) Mantener la documentación de seguridad actualizada y organizada, así como gestionar los mecanismos de acceso a esta.

c) Determinar las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

d) Verificar y supervisar que las medidas de seguridad son adecuadas para la protección de la información y los servicios y proponer las decisiones respecto a las medidas que considere imprescindibles para preservar la seguridad, integridad y disponibilidad de los servicios prestados y la información manejada por el Departamento.

e) Dirigir, coordinar y apoyar la investigación de los incidentes de seguridad desde su detección hasta su resolución, y coordinar la comunicación con el Centro Criptológico Nacional en la utilización de servicios de respuesta a incidentes de seguridad.

f) Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.

cve: BOE-A-2026-1905
Verificable en https://www.boe.es

g) Cualquier otra función en el ámbito de la seguridad de la información y los servicios que le sea encomendada a través de la normativa de seguridad de segundo nivel al respecto.

4. La persona designada como Responsable de la Seguridad no podrá ser designada como Responsable de la Información, ni del Servicio. Adicionalmente, deberá ser distinta de la persona designada Responsable del Sistema y no podrá existir dependencia jerárquica entre ambas. En aquellas situaciones excepcionales en las que la ausencia justificada de recursos haga necesario que la función de Responsable de la Seguridad y la función de Responsable del Sistema recaiga 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 Real Decreto 311/2022, de 3 de mayo.

Igualmente, la persona designada Responsable de la Seguridad no podrá coincidir con la persona designada como Delegada de Protección de Datos y no podrá existir dependencia jerárquica entre ambos a fin de garantizarse la necesaria independencia y ausencia de conflicto de intereses.

5. En casos de vacante, ausencia, enfermedad, abstención, recusación u otra causa legal, la persona designada Responsable de la Seguridad será sustituida por la persona designada por la persona titular de la DTSI, y en su defecto, por la persona de dicha unidad con mayor jerarquía, antigüedad y edad, por este orden.

Artículo 10. *La persona designada Responsable del Sistema.*

1. La persona designada Responsable del Sistema (de información), será nombrada por la persona titular de la DTSI y, de acuerdo con lo previsto en el artículo 13 del Real Decreto 311/2022, de 3 de mayo y en la correspondiente guía CCN-STIC sobre roles y funciones en el ENS, y es la persona encargada de la explotación de los sistemas de información de su ámbito específico de competencias, así como de desarrollar la forma concreta de implementar la seguridad en los sistemas y de la supervisión de la operación diaria de los mismos.

Este ámbito vendrá determinado por los sistemas de información, los tratamientos de datos personales y servicios de tecnologías de la información y de las comunicaciones que sean prestados y/o gestionados directamente por la DTSI.

2. Las funciones que corresponden a la persona designada Responsable del Sistema son:

a) Definir la tipología y sistema de gestión del Sistema de Información, estableciendo los criterios de uso y los servicios disponibles en este.

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

c) Suspender el tratamiento de una determinada información o la prestación de un determinado servicio electrónico si es informado o detecta deficiencias graves de seguridad, previo acuerdo con la persona designada Responsable de la Seguridad y con el conocimiento previo de la persona designada Responsable de dicha Información o de dicho Servicio.

d) Cualquier otra función en el ámbito de la seguridad de los sistemas de información que le sea encomendada a través de la normativa de seguridad de segundo nivel al respecto.

3. La persona designada Responsable del Sistema podrá designar motivadamente, siendo responsable de su actuación, a las personas delegadas como Administradores de los Sistemas que considere necesarios para el adecuado cumplimiento de sus funciones, quienes actuarán bajo su coordinación y de acuerdo con sus criterios.

4. En casos de vacante, ausencia, enfermedad, abstención, recusación u otra causa legal, la persona designada Responsable del Sistema será sustituida por aquel

cve: BOE-A-2026-1905
Verificable en https://www.boe.es

que designe la persona titular de la DTSI, y en su defecto, por la persona del área funcional de la DTSI encargada de la explotación de los sistemas de información con mayor jerarquía, antigüedad y edad, por este orden.

Artículo 11. *Las personas designadas Responsables de la Información.*

1. Las personas designadas Responsables de la Información, de acuerdo con lo previsto en el artículo 13 del Real Decreto 311/2022, de 3 de mayo, y en la correspondiente guía CCN-STIC sobre roles y funciones en el ENS, tienen la potestad, dentro de su ámbito de actuación y competencias, de aprobar los requisitos en materia de seguridad de la información que manejan y, por tanto, de su protección. Si esta información incluye datos de carácter personal, además deberán tenerse en cuenta los requisitos derivados de la legislación correspondiente sobre protección de datos [el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y la Ley Orgánica 3/2018, de 5 de diciembre].

2. Serán funciones de las personas designadas Responsables de la Información, dentro de sus ámbitos de actuación, las siguientes:

a) Determinar los niveles de seguridad de la información tratada valorando los impactos de los incidentes que afecten a la seguridad de la información.

b) Son los encargados, junto a las personas designadas Responsables del Servicios y contando con la participación de la persona designada Responsable de la Seguridad, de realizar los preceptivos análisis de riesgos y seleccionar las salvaguardas que se han de implantar.

c) Son las responsables de aceptar los riesgos residuales respecto de la información, calculados en el análisis de riesgos.

d) Son las responsables últimas de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad de la información tratada dentro de su ámbito de actuación y competencias.

e) Tienen la responsabilidad última del uso y acceso que se haga de la información de la que son responsables y, por tanto, de su mantenimiento y protección.

f) Cualquier otra función en el ámbito de la seguridad de la información que le sea encomendada a través de la normativa de seguridad de segundo nivel al respecto.

3. La designación de las personas Responsables de la Información, con rango mínimo de Subdirector General corresponderá a la persona titular de cada órgano superior o directivo, y de cada organismo público dependiente del Ministerio a los que sea de aplicación esta PSI, de acuerdo con su propia organización interna.

4. En casos de vacante, ausencia, enfermedad, abstención, recusación u otra causa legal, las personas designadas Responsables de la Información serán sustituidas por aquellas que designe la persona titular de cada órgano superior o directivo, y de cada organismo público dependiente del Ministerio a los que sea de aplicación esta PSI, y en su defecto, por la persona del área funcional responsable de la información con mayor jerarquía, antigüedad y edad, por este orden.

Artículo 12. *Las personas designadas Responsables del Servicio.*

1. Las personas designadas como Responsables del Servicio, de acuerdo con lo previsto en el artículo 13 del Real Decreto 311/2022, de 3 de mayo, y en la correspondiente guía CCN-STIC sobre roles y funciones en el ENS, tienen la potestad, dentro de su ámbito de actuación y competencias, de aprobar los requisitos en materia de seguridad de los servicios que prestan y, por tanto, de determinar los niveles de seguridad de dichos servicios.

cve: BOE-A-2026-1905
Verificable en https://www.boe.es

2. Serán funciones de las personas designadas Responsables del Servicio, dentro de sus ámbitos de actuación, las siguientes:

a) Determinar los niveles de seguridad de los servicios prestados valorando los impactos de los incidentes que afecten a la seguridad del servicio.
b) Son las encargadas, junto a las personas designadas Responsables de la Información y contando con la participación de la persona designada Responsable de la Seguridad, de realizar los preceptivos análisis de riesgos y seleccionar las salvaguardas que se han de implantar.
c) Son las responsables de aceptar los riesgos residuales respecto de los servicios calculados en el análisis de riesgos.
d) Cualquier otra función en el ámbito de la seguridad de los servicios que le sea encomendada a través de la normativa de seguridad de segundo nivel al respecto.

3. La designación de las personas Responsables del Servicio, con rango mínimo de Subdirector General corresponderá a la persona titular de cada órgano superior o directivo del Departamento, y de cada organismo público dependiente del Ministerio a los que sea de aplicación esta PSI, de acuerdo con su propia organización interna.
4. En casos de vacante, ausencia, enfermedad, abstención, recusación u otra causa legal, las personas designadas Responsables del Servicio serán sustituidas por aquellas que designe la persona titular de cada órgano superior o directivo, y de cada organismo público dependiente del Ministerio a los que sea de aplicación esta PSI, y en su defecto, por la persona del área funcional responsable del servicio con mayor jerarquía, antigüedad y edad, por este orden.

Artículo 13. *La persona designada Delegada de Protección de Datos.*

1. El DPD desempeñará las funciones detalladas en la sección 4 del capítulo IV del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y en el título V, capítulo III de la Ley Orgánica 3/2018, de 5 de diciembre, y demás disposiciones reguladoras de la materia.
La actuación del DPD se regirá por el principio de independencia, por lo que no recibirán ninguna instrucción en lo que respecta al desempeño de sus funciones. Podrán estar asistidos por grupos de trabajo integrados por representantes de las unidades administrativas de su ámbito de actuación.
2. A fin de garantizar su independencia y evitar cualquier tipo de conflicto de intereses en el ejercicio de sus funciones, no podrá coincidir en la misma persona la designación del DPD y la persona designada Responsable de la Seguridad. Así mismo, entre las personas designadas para los citados cargos, no existirá ningún tipo de dependencia funcional u orgánica.

Artículo 14. *Protección de datos de carácter personal.*

1. En el ámbito del Ministerio de Juventud e Infancia, la garantía de la protección de datos de carácter personal de las actividades de tratamiento es un objetivo compartido por todas las unidades del Departamento que se rige por los principios recogidos en el artículo 5 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.
2. La seguridad de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, constituye uno de los principios que deben regir su tratamiento, aplicándose para ello las medidas técnicas u organizativas apropiadas que garanticen un nivel de seguridad adecuado en función del correspondiente análisis de riesgos, tal y como se establece en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y en la Ley Orgánica 3/2018, de 5 de diciembre. Dicho análisis de riesgos se realizará, teniendo en cuenta el estado de la técnica, los costes de aplicación, la

cve: BOE-A-2026-1905
Verificable en https://www.boe.es

naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas.

El cumplimiento de este principio corresponde al Responsable del tratamiento que, adicionalmente, debe ser capaz de demostrarlo y aplicarlo de forma temprana en la fase de diseño del tratamiento y garantizando que su aplicación sea efectiva por defecto.

3. La garantía del cumplimiento de lo previsto en el apartado anterior, se articulará a través del marco organizativo establecido en la presente Política de Seguridad y se llevará a cabo de conformidad con la normativa aplicable en materia de protección referida en el artículo 2 de esta orden y en el Real Decreto 311/2022, de 3 de mayo, prevaleciendo las medidas derivadas de la aplicación de la normativa de protección de datos cuando, tras un análisis de riesgos, se estime que las mismas son superiores a las previstas en el ENS.

4. La observación del principio de seguridad del tratamiento de los datos personales cobrará especial relevancia cuando sea probable que un determinado tratamiento entrañe un alto riesgo para los derechos y libertades de las personas físicas, en cuyo caso el Responsable del tratamiento recabará el asesoramiento del DPD al realizar la preceptiva evaluación de impacto relativa a la protección de datos.

5. Las auditorías de seguridad previstas en el Esquema Nacional de Seguridad incorporarán la revisión de las medidas técnicas y organizativas de seguridad de los datos personales a las que se refiere este artículo.

Artículo 15. *Resolución de conflictos.*

La resolución de los conflictos que puedan derivarse del establecimiento de la estructura organizativa de seguridad corresponderá al superior jerárquico su solución si pertenecen al mismo órgano superior del departamento. En otro caso, así como aquellos conflictos de competencia que pudieran aparecer entre los diferentes centros directivos en materia de seguridad de la información, corresponderá al CSID.

Disposición adicional primera. *Política de seguridad de la información de los organismos y entidades vinculados, dependientes o adscritos al Ministerio de Juventud e Infancia.*

1. De acuerdo con lo previsto en el artículo 12.3 del Real Decreto 311/2022, de 3 de mayo, y el artículo 1.2 de esta orden, los organismos y entidades vinculados, dependientes o adscritos al Ministerio de Juventud e Infancia podrán contar con su propia política de seguridad, aprobada por el 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 públicos o entidades vinculados o dependientes del Departamento deberán informar de forma inmediata a la División de Tecnologías de la Innovación sobre cualquier incidencia o riesgo que pueda poner en peligro la seguridad de los sistemas informáticos del Departamento.

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

La aplicación de esta orden no conllevará incremento del gasto público, ni supondrá incremento de dotaciones, ni de retribuciones u otros gastos de personal.

Disposición adicional tercera. *Actualización permanente y revisiones periódicas de la PSI.*

1. Esta orden deberá mantenerse actualizada para adecuarla al progreso de los servicios de la Administración Digital, a la evolución tecnológica y al desarrollo de la sociedad de la información.

2. Las propuestas de las sucesivas revisiones de la PSI corresponden al CSID.

cve: BOE-A-2026-1905
Verificable en https://www.boe.es

Disposición adicional cuarta. *Deber de colaboración en la implantación de la PSI.*

Todos los órganos y unidades del Departamento y de sus organismos públicos prestarán su colaboración en las actuaciones de implementación de la PSI aprobada por esta orden.

Disposición derogatoria única. *Derogación normativa.*

Quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo establecido en esta orden.

Disposición final primera. *Instrucciones de ejecución.*

La persona titular de la Subsecretaría de Juventud e Infancia podrá dictar las instrucciones necesarias para la ejecución y aplicación de esta orden, de conformidad con lo previsto en el artículo 6 de la Ley 40/2015, de 1 de octubre.

Disposición final segunda. *Publicidad de la PSI.*

Esta orden se publicará en el portal de internet y en la sede del Ministerio de Juventud e Infancia (www.Juventudeinfancia.gob.es, y https://juventudeinfancia.sede.gob.es/).

Disposición final tercera. *Entrada en vigor.*

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

Disposición final cuarta. *Vigencia.*

La presente orden, así como su marco normativo aprobado, seguirá vigente en tanto en cuanto no sea aprobada la política de seguridad del departamento ministerial que asuma las competencias del Ministerio de Juventud e Infancia y se desarrolle la estructura normativa que garantice la seguridad de los activos tecnológicos y de información utilizados por los órganos u organismos comprendidos en el ámbito subjetivo de la presente PSI para el ejercicio de sus competencias.

Madrid, 14 de enero de 2026.–La Ministra de Juventud e Infancia, Sira Abed Rego.

cve: BOE-A-2026-1905
Verificable en https://www.boe.es