

III. OTRAS DISPOSICIONES

MINISTERIO DE JUVENTUD E INFANCIA

22784 *Resolución de 8 de octubre de 2026, del Instituto de la Juventud, O.A., por la que se aprueba la Política de Seguridad de la Información en el ámbito de la administración electrónica del organismo.*

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 (ENI) 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 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, dispone que, en la Administración General del Estado, cada ministerio contará con su política de seguridad. Los organismos públicos y entidades pertenecientes al sector público institucional estatal podrán contar con su propia política de seguridad, aprobada por el órgano competente, que será coherente con la del departamento con el que mantenga la relación de vinculación, dependencia o adscripción, o bien quedar comprendidos en el ámbito subjetivo de la política de seguridad de éste.

En este sentido, el organismo autónomo Instituto de la Juventud (en adelante, INJUVE) se encuentra adscrito al Ministerio de Juventud e Infancia, cuya política de seguridad quedó aprobada mediante 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.

Por su parte, el INJUVE, para el desarrollo y cumplimiento de las funciones y objetivos que se le atribuyen ha situado los sistemas de Tecnologías de la Información y de las Comunicaciones (TIC) como elementos estratégicos, especialmente en un entorno de amenazas digitales en constante evolución y de distinta naturaleza. A tenor de una sociedad con gran exposición digital, la gestión de la seguridad y de la información se convierte en una necesidad para lograr su protección frente a las amenazas que puedan afectar a su autenticidad, integridad, disponibilidad, confidencialidad y trazabilidad.

En consecuencia, la presente resolución tiene por objeto establecer la Política de Seguridad de la Información en el ámbito de la administración electrónica del INJUVE, así como establecer la estructura organizativa para definirla, implantarla y gestionarla, garantizando en todo caso la coherencia con la Política de Seguridad de la Información del departamento de adscripción.

Durante su tramitación, se han recabado los informes de la Comisión Ministerial de Administración Digital del Ministerio de Juventud e Infancia y de la persona designada Delegado de Protección de Datos del INJUVE.

En virtud de lo expuesto, resuelvo:

Primero. *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 en al ámbito de la Administración Electrónica, constituye el objeto de la presente resolución la aprobación de la Política de Seguridad de la Información (en adelante, PSI) en el ámbito de la Administración Digital del Instituto de la Juventud (en adelante, INJUVE), así como del marco organizativo global en materia de Seguridad de la Información del organismo autónomo.

2. La PSI será de obligado cumplimiento para todas las unidades del organismo autónomo.

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 organismo autónomo, con independencia de cuál sea su destino, adscripción o relación con éste.

Segundo. *Misión del organismo autónomo.*

El INJUVE, de acuerdo con el Real Decreto 608/2025, de 8 de julio, por el que se aprueba el Estatuto del organismo autónomo Instituto de la Juventud, es el organismo de la Administración General del Estado al que corresponde la política del Gobierno en materia de juventud como ente vertebrador del conocimiento de la realidad juvenil a nivel estatal y de la participación de las personas jóvenes en la elaboración de las políticas públicas a este nivel, así como interlocutor frente a la Unión Europea en esta materia.

Tercero. *Marco normativo.*

1. El marco normativo en que se desarrollan las actividades del INJUVE 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 el 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 608/2025, de 8 de julio, por el que se aprueba el Estatuto del organismo autónomo Instituto de la Juventud.
- 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.
- q) 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.
- r) 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.
- s) La Ley 9/1968, de 5 de abril, sobre secretos oficiales.
- t) La Resolución de 18 de noviembre de 2025, del Instituto de la Juventud, O.A., por la que se crea la sede electrónica del organismo.

2. Del mismo modo, las actuaciones que desarrolle el INJUVE en aplicación de la presente resolución se adecuarán a las normas aplicables a la Administración Electrónica del organismo autónomo que desarrollen o complementen las disposiciones normativas citadas en el apartado anterior vinculadas al ámbito de aplicación de la PSI.

Cuarto. *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.

Quinto. *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 resolución.
- 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 organismo autónomo 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 organismo autónomo. Este ámbito vendrá determinado por los sistemas de información y servicios TIC que sean prestados y gestionados directamente por este organismo autónomo. En otro caso, se entienden de obligado conocimiento y cumplimiento por parte de toda persona que acceda a dichos servicios la PSI del departamento, organismo público o entidad competente, así como los desarrollos normativos de segundo nivel correspondientes a dichos servicios TIC no prestados o gestionados directamente por el INJUVE.

Las normas y directrices generales de seguridad de este segundo nivel normativo serán aprobadas por resolución de la persona titular de la Dirección General del INJUVE, a propuesta del Comité de Seguridad de la Información del INJUVE.

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 INJUVE. 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 organismo autónomo. En otro caso, se entienden de obligado conocimiento y cumplimiento por parte de toda persona que acceda a dichos servicios la PSI del departamento, organismo público o entidad competente, así como los desarrollos normativos de tercer nivel correspondientes a dichos servicios TIC no prestados o gestionados directamente por el INJUVE.

Su aprobación corresponde a la persona responsable de la seguridad, previo acuerdo en el Comité de Seguridad de la Información del INJUVE.

2. La normativa interna de seguridad podrá incorporar asimismo otros instrumentos tales como estándares de seguridad, buenas prácticas, informes técnicos, a criterio del INJUVE, siempre dentro del ámbito de sus competencias y responsabilidades.

3. El personal de cada una de las unidades del INJUVE 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 del INJUVE a través de una sección diferenciada en la intranet del mismo.

Sexto. *Estructura organizativa.*

1. La organización de la seguridad debe tener en cuenta la propia organización del organismo autónomo, en consecuencia, las responsabilidades en seguridad de la información deben emerger de todas las unidades del mismo, 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 INJUVE está compuesta por los siguientes agentes:

- a) La persona titular de la Dirección General.
- b) El Comité de Seguridad de la Información del INJUVE.
- 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) La persona designada como Delegada de Protección de Datos del organismo autónomo.
- g) Las personas designadas como Administradores de Sistemas.

Séptimo. *Competencias de la persona titular de la Dirección General del INJUVE en el ámbito de la Seguridad de la Información.*

La persona titular de la Dirección General del INJUVE 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 Dirección General, 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 INJUVE.
- d) Será responsable de promover la mejora continua en la gestión de la seguridad de la información en el ámbito del INJUVE.

Octavo. *El Comité de Seguridad de la Información del INJUVE.*

1. Con carácter permanente, se crea el Comité de Seguridad de la Información del INJUVE (en adelante, CSI) con el objeto de dotar al organismo autónomo 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 CSI estará compuesto por las siguientes personas:

a) Presidencia: Corresponderá a la persona titular de la Secretaría General. Tendrá voz y voto de calidad en la toma de decisiones del CSI. 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 organismo.

3.º Las personas designadas como Delegada de Protección de Datos del INJUVE. 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 las personas designadas Delegadas de Protección de Datos si no coinciden con la decisión adoptada por el CSI.

c) Secretaría: Corresponderá a la persona designada como Responsable de la Seguridad del organismo autónomo, que tendrá voz y voto y que ejecutará las decisiones del CSI, 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 unidad que accedan a sistemas de información del organismo autónomo, 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, la persona titular de la Presidencia será sustituido por aquella que designe la persona titular de la Dirección General. En el caso de las vocalías, éstas serán sustituidas por aquellos representantes que éstas designen.

5. El CSI 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 CSI:

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

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 el INJUVE, 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 apartado cuarto, 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 organismo autónomo, 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 Dirección General 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 CSI.

8. El CSI se regirá por las normas de funcionamiento previstas en la presente resolución 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.

Noveno. *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 Secretaría General 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 organismo autónomo, 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 CSI.
- 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 organismo autónomo.
- 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.
- 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 Secretaría General, y en su defecto, por la persona de dicha unidad con mayor jerarquía, antigüedad y edad, por este orden.

Décimo. La persona designada Responsable del Sistema de Información.

1. La persona designada Responsable del Sistema, será nombrada por la persona titular de Secretaría General 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 Secretaría General.

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

Undécimo. *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 de los 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, se realizará entre personal funcionario de carrera de, al menos, un nivel 26 de complemento de destino y corresponderá a la persona titular de la Secretaría General.

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 la Secretaría General, y en su defecto, por la persona del área funcional responsable de la información con mayor jerarquía, antigüedad y edad, por este orden.

Duodécimo. 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.

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, que se realizará entre personal funcionario de carrera de, al menos, un nivel 26 de complemento de destino, corresponderá a la persona titular de la Secretaría General.

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 la Secretaría General, y en su defecto, por la persona del área funcional responsable del servicio con mayor jerarquía, antigüedad y edad, por este orden.

Decimotercero. 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.

Su designación debe efectuarse de conformidad con lo dispuesto en el artículo 37 del Reglamento (UE) 2016/679 y en el artículo 34 de la Ley Orgánica 3/2018, de 5 de diciembre, atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y de la práctica en materia de protección de datos, así como a su capacidad para desempeñar las funciones que tiene encomendadas.

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.

Decimocuarto. *Protección de datos de carácter personal.*

1. En el ámbito del INJUVE, la garantía de la protección de datos de carácter personal de las actividades de tratamiento es un objetivo compartido por todas las unidades del mismo 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 y 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 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.

En los tratamientos de datos personales se identificará a la persona, organismo o unidad responsable de tratamiento y, en su caso, al encargado de tratamiento, de acuerdo con lo dispuesto en el artículo 4, apartados 7 y 8 del mencionado reglamento.

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 resolución 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, conforme al artículo 35 del RGPD y los criterios establecidos por la Agencia Española de 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.

Decimoquinto. *Resolución de conflictos.*

La resolución de los conflictos que puedan derivarse del establecimiento de la estructura organizativa de seguridad corresponderá al superior jerárquico si pertenecen al mismo órgano superior del INJUVE. 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 CSI.

Las discrepancias entre el CSI del organismo y los órganos equivalentes del departamento de adscripción serán elevadas para su resolución al órgano competente del departamento.

Decimosexto. *Relación con la política de seguridad de la información del departamento de adscripción.*

1. El INJUVE realizará las adaptaciones oportunas de su PSI al efecto de garantizar el adecuado alineamiento con la política de seguridad de la información del departamento de adscripción.

La presente Política de Seguridad de la Información se aplicará de forma coherente con la Política de Seguridad de la Información del Ministerio de Juventud e Infancia aprobada por Orden JUI/29/2026, de 14 de enero. En caso de discrepancia prevalecerá la política departamental.

2. Ante el supuesto de incidencias o riesgos que pueda poner en peligro la seguridad de los sistemas informáticos del departamento, el Instituto de la Juventud informará del asunto a la unidad competente en materia de seguridad de información del Ministerio de adscripción.

Cuando existan servicios TIC compartidos con el departamento de adscripción se establecerán mecanismos de coordinación entre los CSI de ambos, así como procedimientos conjuntos de respuesta ante incidentes de seguridad.

Se plantea a nivel operativo, como vía para cubrir esta necesidad de coordinación y armonización de normativa y actuaciones en materia de seguridad, la constitución de un Grupo de Trabajo en materia de Seguridad de la Información, en el que los presidentes de ambos Comités y/o los Responsables de Seguridad de ambos organismos se reúnan para revisar estos aspectos de coordinación entre los dos organismos en relación con sus políticas, conforme a lo estipulado en el artículo 8.3. de la PSI del Ministerio de Juventud e Infancia.

Decimoséptimo. *No incremento del gasto público.*

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

Decimoctavo. *Actualización permanente y revisiones periódicas de la Política de Seguridad de la Información.*

La Política de Seguridad de la Información del Instituto de la Juventud 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.

Las propuestas de las sucesivas revisiones de la Política de Seguridad de la Información corresponden al Comité de Seguridad de la Información.

Decimonoveno. *Deber de colaboración en la implantación de la Política de Seguridad de la Información.*

Todas las unidades del INJUVE prestarán su colaboración en las actuaciones de implementación de la Política de Seguridad de la Información aprobada por esta resolución.

Vigésimo. *Instrucciones de ejecución.*

La persona titular de la Dirección General podrá dictar las instrucciones necesarias para la ejecución y aplicación de esta resolución, de conformidad con lo previsto en el artículo 6 de la Ley 40/2015, de 1 de octubre.

Vigesimoprimer. *Efectos.*

Esta resolución surtirá efectos el día siguiente al de su publicación en el «Boletín Oficial del Estado».

Madrid, 8 de octubre de 2026. –La Directora General del Instituto de la Juventud, Margarita del Cisne Guerrero Calderón.