III. OTRAS DISPOSICIONES

MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA

13777 *Orden HFP/873/2021, de 29 de julio, por la que se aprueba la Política de Seguridad de la Información en el ámbito de la Administración digital del Ministerio de Hacienda y Función Pública*

El marco de relación entre la Administración Pública y los ciudadanos a través de los medios electrónicos se encuentra establecido en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Por su parte, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, define en su artículo 156 el objeto del Esquema Nacional de Seguridad (ENS) y lo incorpora como parte esencial en la configuración del archivo electrónico de los documentos regulado en el artículo 46 y en el régimen de relaciones electrónicas y transferencias de tecnología entre las Administraciones Públicas, tal como establece el artículo 158 de esta norma.

Ambas normas han sido objeto de desarrollo en virtud del Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.

La Administración Digital debe ser confiable para que los ciudadanos realicen los trámites administrativos correspondientes con total seguridad y fiabilidad. Para ello, el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (en adelante ENS) en el ámbito de la Administración Digital, persigue fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar a conocimiento de personas no autorizadas.

La Política de Seguridad de la Información constituye el marco de referencia orientado a facilitar la definición, gestión, administración e implementación de los mecanismos y procedimientos de seguridad establecidos en el ENS.

Del mismo modo, determina que la Política de Seguridad de la Información debe ser coherente con lo establecido en el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (Reglamento General de Protección de Datos) y la normativa vigente en esta materia, en lo que corresponda, prevaleciendo lo relativo a la protección de datos de carácter personal en caso de discrepancias.

La Orden HAP/1953/2014, de 15 de octubre, aprobó la política de seguridad de la información en el ámbito de la administración electrónica del Ministerio de Hacienda y Administraciones Públicas. Las modificaciones introducidas en la estructura del ministerio en virtud del Real Decreto 689/2020, de 21 de julio, por el que se desarrolla la estructura orgánica básica del Ministerio de Hacienda y se modifica el Real Decreto 139/2020, de 28 de enero, por el que se establece la estructura orgánica básica de los departamentos ministeriales, junto a la conveniencia de incorporar previsiones en relación con la protección de datos de carácter personal y la política de continuidad de negocio aconsejan la aprobación de la presente orden ministerial que deroga aquella.

Adicionalmente, se ha tenido en cuenta que el recientemente aprobado Real Decreto 507/2021, de 10 de julio, por el que se modifica el Real Decreto 2/2020, de 12 de enero, por el que se reestructuran los departamentos ministeriales, ha modificado la denominación del ministerio, denominándolo Ministerio de Hacienda y Función Pública, e incorporado a su estructura a la Secretaría de Estado de Función Pública.

Esta norma se ajusta a los principios de buena regulación contenidos en el artículo 129 de la Ley 39/2015, de 1 de octubre. En particular, a los principios de necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia y eficiencia.

cve: BOE-A-2021-13777
Verificable en https://www.boe.es

La incorporación de las previsiones relativas a protección de datos al ámbito de la Política de Seguridad de la Información (PSI) del Ministerio de Hacienda y Función Pública pretende favorecer el cumplimiento en el Departamento de las previsiones contenidas en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, considerándose de acuerdo con el principio de eficiencia que es el instrumento más adecuado para el logro de dicho objetivo.

El fundamento jurídico del proyecto se encuentra en el artículo 11 del Real Decreto 3/2010, de 8 de enero, que establece que todos los órganos superiores de las Administraciones públicas deberán disponer formalmente de su política de seguridad que articule la gestión continuada de la seguridad, que será aprobada por el titular del órgano superior correspondiente, lo que enlaza con los principios de necesidad, seguridad jurídica y transparencia.

De acuerdo con los principios de eficacia y eficiencia, el proyecto mantiene la estructura organizativa preexistente en relación con la Política de Seguridad de la Información (PSI) en el Ministerio de Hacienda y Función Pública e incluye, adicionalmente, las cuestiones relativas a protección de datos personales y política de continuidad de negocio.

De la norma proyectada no se derivan impactos apreciables en el orden económico, presupuestario, de distribución de competencias, ni por razón de género, tratándose de una modificación puntual de una norma de carácter organizativo en el ámbito de la Administración General del Estado, con lo que se da cumplimiento al principio de proporcionalidad.

Esta orden ha sido informada por la Comisión Ministerial de Administración Digital y la Agencia Española de Protección de Datos.

En su virtud, dispongo:

Artículo 1. *Objeto y ámbito de aplicación.*

1. 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 Hacienda y Función Pública, así como su marco organizativo y tecnológico.

2. La PSI será de obligado cumplimiento para todos los órganos superiores y directivos del Ministerio de Hacienda y Función Pública, incluidos los órganos territoriales adscritos al Ministerio, que no tengan establecida su propia política de seguridad, siendo aplicable a los activos empleados por el Departamento en la prestación de los servicios de la Administración Digital.

3. Se podrán adscribir a la presente PSI aquellos organismos y entidades de derecho público vinculados o dependientes del Ministerio de Hacienda y Función Pública que no tengan establecida su propia política de seguridad y así lo soliciten.

4. La PSI será de obligado cumplimiento para todo el personal que acceda tanto a los sistemas de información como a la propia información que sea gestionada por el Departamento, con independencia de cuál sea su destino, adscripción o relación.

Artículo 2. *Misión del Departamento.*

El Ministerio de Hacienda y Función Pública es el Departamento de la Administración General del Estado encargado de la propuesta y ejecución de la política del Gobierno en las siguientes materias: hacienda pública, presupuestos y gastos, administración pública, función pública y gobernanza pública, empresas públicas, aplicación y gestión de los sistemas de financiación autonómica y local, provisión de información sobre la actividad económico-financiera de las distintas administraciones públicas y estrategia, coordinación y normativa en materia de contratación pública.

cve: BOE-A-2021-13777
Verificable en https://www.boe.es

Artículo 3. *Marco legal y regulatorio.*

El marco normativo en que se desarrollan las actividades del Ministerio de Hacienda y Función Pública en el ámbito de la prestación de los servicios electrónicos a los ciudadanos, sin perjuicio de la legislación específica, se compone de:

1. 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).
2. Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
3. Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.
4. Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
5. Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
6. 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.
7. 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.
8. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
9. Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.
10. 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.
11. 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.
12. Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en al ámbito de la Administración Electrónica y las Instrucciones Técnicas de Seguridad dictadas para su aplicación.
13. 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 y las Normas Técnicas de Interoperabilidad dictadas su aplicación.
14. Orden HAP/548/2013, de 2 de abril, por la que se crean y regulan sedes electrónicas en el Ministerio de Hacienda y Administraciones Públicas.
15. Orden HAP/547/2013, de 2 de abril, por la que se crea y se regula el Registro Electrónico del Ministerio de Hacienda y Administraciones Públicas.

Del mismo modo, forman parte del marco regulatorio las normas aplicables a la Administración Electrónica del Departamento que desarrollen o complementen las anteriores y que se encuentren dentro del ámbito de aplicación de la PSI.

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

1. Principios básicos.

Los principios básicos son directrices fundamentales de seguridad que han de tenerse siempre presentes en cualquier actividad relacionada con el uso de los activos de información. Se establecen los siguientes:

a) Alcance estratégico: La seguridad de la información debe contar con el compromiso y apoyo de todos los niveles directivos de forma que pueda estar

cve: BOE-A-2021-13777
Verificable en https://www.boe.es

coordinada e integrada con el resto de iniciativas estratégicas del Departamento para conformar un todo coherente y eficaz.

b) Responsabilidad diferenciada: En los sistemas de información se diferenciará el responsable de la información, que determina los requisitos de seguridad de la información tratada; el responsable del servicio, que determina los requisitos de seguridad de los servicios prestados; el responsable del sistema, que tiene la responsabilidad sobre la prestación de los servicios; y el responsable de seguridad, que determina las decisiones para satisfacer los requisitos de seguridad. En los supuestos de tratamientos de datos personales además se identificará el responsable de tratamiento y, en su caso, el encargado de tratamiento, de acuerdo con el artículo 12 de esta Orden.

c) Seguridad integral: La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas de información.

d) Gestión de Riesgos: El análisis y gestión de riesgos será parte esencial del proceso de seguridad. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad. El análisis y gestión de riesgos, cuando se aplique al tratamiento de datos personales, tendrá especial consideración con los riesgos para los derechos y libertades de las personas físicas.

e) Proporcionalidad: El establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.

f) Mejora continua: Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado, instruido y dedicado.

g) Seguridad por defecto: Los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad y protección de datos personales por defecto y desde el diseño.

2. Principios particulares.

Las directrices fundamentales de seguridad se concretan en un conjunto de principios particulares y responsabilidades específicas, que se configuran como objetivos instrumentales que garantizan el cumplimiento de los principios básicos de la PSI y que inspiran las actuaciones del Departamento en dicha materia. Se establecen los siguientes:

a) Protección de datos de carácter personal: se adoptarán las medidas técnicas y organizativas destinadas a garantizar y poder demostrar que la seguridad del tratamiento es conforme con la normativa vigente en materia de protección de datos personales

b) Gestión de activos de información: Los activos de información del Departamento se encontrarán inventariados y categorizados y estarán asociados a un responsable.

c) Seguridad ligada a las personas: se implantarán los mecanismos necesarios para que cualquier persona que acceda o pueda acceder a los activos de información, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos.

d) Seguridad física: Los activos de información serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad.

cve: BOE-A-2021-13777
Verificable en https://www.boe.es

Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.

e) Seguridad en la gestión de comunicaciones y operaciones: se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las Tecnologías de la Información y Comunicaciones. La información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.

f) Control de acceso: se limitará el acceso a los activos de información por parte de usuarios, procesos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo. Además, quedará registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso y auditar su uso adecuado, conforme a la actividad de la organización.

g) Adquisición, desarrollo y mantenimiento de los sistemas de información: se contemplarán los aspectos de seguridad de la información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.

h) Gestión de los incidentes de seguridad: se implantarán los mecanismos apropiados para la correcta identificación, registro, notificación y resolución de los incidentes de seguridad.

i) Gestión de la continuidad: se implantarán los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de sus procesos de negocio, de acuerdo a las necesidades de nivel de servicio de sus usuarios.

j) Cumplimiento: se adoptarán las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información y protección de datos personales.

Artículo 5. *Estructura organizativa.*

La estructura organizativa para la gestión de la seguridad de la información en el ámbito descrito por la PSI del Ministerio de Hacienda y Función Pública está compuesta por los siguientes agentes:

1. El Comité de Dirección de Seguridad de la Información.
2. El Grupo de trabajo Técnico de Seguridad de la Información.
3. Los Responsables de Seguridad.
4. Los Responsables de la Información.
5. Los Responsables del Servicio.
6. Los Responsables del Sistema.
7. El Delegado de la Protección de Datos del departamento y los Delegados de Protección de Datos de los organismos públicos adscritos al departamento.

Artículo 6. *El Comité de Dirección de Seguridad de la Información.*

1. El Comité de Dirección de Seguridad de la Información (en adelante CDSI), adscrito a la Subsecretaría del Ministerio de Hacienda y Función Pública, está compuesto por los siguientes miembros:

a) Presidente: La persona titular de la Subsecretaría del Ministerio de Hacienda y Función Pública.

b) Vicepresidente Primero: La persona titular de la Inspección General del Ministerio de Hacienda y Función Pública.

c) Vicepresidente Segundo: La persona titular del Departamento de Servicios y Coordinación Territorial.

cve: BOE-A-2021-13777
Verificable en https://www.boe.es

d) Vocales:

1.º Dos representantes de la Secretaría de Estado de Hacienda, nombrados por el titular de dicho órgano superior, de los que al menos uno de ellos tenga rango mínimo de director general y el otro con rango mínimo de subdirector general.

2.º Dos representantes de la Secretaría de Estado de Presupuestos y Gastos, nombrados por el titular de dicho órgano superior, de los que al menos uno de ellos tenga rango mínimo de director general y el otro con rango mínimo de subdirector general.

3.º Dos representantes de la Secretaría de Estado de Función Pública, nombrados por el titular de dicho órgano superior, de los que al menos uno de ellos tenga rango mínimo de director general y el otro con rango mínimo de subdirector general.

4.º Un representante de la Intervención General de la Administración del Estado, nombrado por el titular de dicho órgano, con rango mínimo de subdirector general.

5.º La persona titular de la Subdirección General de Tecnologías de la Información y de las Comunicaciones, que actuará como Secretario.

6.º El Delegado de Protección de Datos del departamento, que participará con voz pero sin voto, haciéndose constar en acta su parecer si no coincide con la decisión adoptada por el CDSI.

2. El CDSI ejercerá las siguientes funciones:

a) Aprobar las propuestas de modificación y actualización permanente que se hagan sobre la PSI.

b) Aprobar el resto de la normativa de seguridad de primer nivel definida en el artículo 15.

c) Velar e impulsar el cumplimiento de la PSI y de su desarrollo normativo.

d) Promover la mejora continua en la gestión de la seguridad de la información y la protección de datos personales.

e) Seguimiento del estado de la política de continuidad del negocio e impulso de su mejora

f) Resolver los posibles conflictos que puedan derivarse del establecimiento de la citada estructura organizativa.

3. El CDSI se reunirá con carácter ordinario al menos una vez al año, y con carácter extraordinario cuando lo decida su Presidente y las sesiones se celebrarán de forma presencial o a distancia, lo que se especificará necesariamente en la convocatoria.

4. El CDSI podrá recabar del personal técnico, propio o externo, la información pertinente para la toma de sus decisiones.

5. En lo no previsto en esta Orden, el funcionamiento del CDSI se ajustará a lo dispuesto en materia de órganos colegiados por la sección 3.ª del capítulo II del título preliminar de la Ley 40/2015, de 1 de octubre.

Artículo 7. *Grupo de trabajo Técnico de Seguridad de la Información.*

1. El «Grupo de Trabajo Técnico de Seguridad de la Información» (GTTSI en adelante), dependiente del CDSI, es competente, con carácter permanente, para conocer las cuestiones técnicas que deban de abordarse en relación con la PSI.

2. El GTTSI estará compuesto por los siguientes miembros: el titular de la Subdirección General de Tecnologías de la Información y de las Comunicaciones, un Inspector de los Servicios, los responsables de Seguridad definidos en el artículo 8 y el Delegado de Protección de Datos ministerial. Asimismo, y con el fin de asegurar la coordinación en materia de seguridad de la información con el conjunto del Ministerio y con otras instancias de la AGE, el GTTSI contará con la participación del responsable de del seguridad de la Agencia Estatal de la Administración Tributaria y, en el mismo, podrán participar representantes de órganos superiores o directivos del Ministerio de

cve: BOE-A-2021-13777
Verificable en https://www.boe.es

Hacienda y Función Pública y organismos y entidades de derecho público vinculados o dependientes Departamento a las que no les sea de aplicación la PSI.

3. El GTTSI colaborará con el CDSI en las cuestiones que éste le encomiende y, de forma particular le corresponderá:

a) Elaborar estudios, análisis previos y propuestas de modificación y actualización de la PSI.

b) Elaborar estudios, análisis previos y propuestas para el resto de la normativa de seguridad de primer nivel definida en el artículo 15.

c) Analizar el cumplimiento de la PSI y de su desarrollo normativo.

d) Analizar las medidas de seguridad de la información, de protección de datos personales y de los servicios electrónicos prestados por los sistemas de información.

e) Analizar el estado de la política de continuidad del negocio.

f) Estudiar las actividades de concienciación y formación en materia de seguridad.

4. El GTTSI se reunirá con carácter ordinario con una frecuencia mínima de dos veces al año y máxima de cuatro, y con carácter extraordinario cuando lo decida el presidente del CDSI. Las sesiones se celebrarán de forma presencial o a distancia, lo que se especificará necesariamente en la convocatoria.

5. En lo no previsto en esta Orden el funcionamiento del grupo de trabajo se ajustará a lo dispuesto en materia de órganos colegiados por la sección 3.ª del capítulo II del título preliminar de la Ley 40/2015, de 1 de octubre.

Artículo 8. *Los Responsables de Seguridad.*

1. Conforme al artículo 10 del ENS, el Responsable de Seguridad es la persona que determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

Cada órgano superior o directivo del Ministerio de Hacienda y Función Pública, así como cada organismo o entidad de derecho público vinculado o dependiente del Departamento a los que sea de aplicación la presente PSI designará un Responsable de Seguridad, sin que, de acuerdo con lo previsto en la disposición adicional primera de la presente Orden, implique, en ningún caso, un aumento de las actuales dotaciones ni de las retribuciones de dichos efectivos por ningún concepto.

2. El ámbito de actuación de cada Responsable de Seguridad se limitará única y exclusivamente a los sistemas de información y servicios de tecnologías de la información y de las comunicaciones que sean competencia y responsabilidad directa del centro o centros para los que haya sido designado Responsable de Seguridad.

3. Serán funciones de cada Responsable de Seguridad, dentro del ámbito de actuación enunciado en el punto anterior, las siguientes:

a) Promover la seguridad de la información manejada, la protección de datos personales y de los servicios electrónicos prestados por los sistemas de información.

b) Elaborar la normativa de seguridad de segundo y tercer nivel definida en el artículo 15.

c) Velar e impulsar el cumplimiento del cuerpo normativo definido en el artículo 15.

d) Encargarse de que la documentación de seguridad se mantenga organizada y actualizada, y de gestionar los mecanismos de acceso a dicha documentación.

e) Promover la mejora continua en la gestión de la seguridad de la información.

f) Impulsar la formación y concienciación en materia de seguridad de la información.

g) Cualesquiera otras funciones que el Real Decreto 3/2010, de 8 de marzo, asigne a los responsables de seguridad.

cve: BOE-A-2021-13777
Verificable en https://www.boe.es

Artículo 9. *Los Responsables de la Información y los Responsables del Servicio.*

1. Los Responsables de la Información tienen la potestad, dentro de su ámbito de actuación y de sus competencias, de establecer los requisitos de la información que manejan y, por lo tanto, de su protección.

2. Los Responsables del Servicio tienen la potestad, dentro de su ámbito de actuación y de sus competencias, de establecer los requisitos del servicio en materia de seguridad y, por tanto, la potestad de determinar los niveles de seguridad del servicio

3. Si la información manejada incluye datos de carácter personal, los Responsables de la Información y los Responsables del Servicio deberán tener en cuenta, además, los requisitos derivados de la legislación correspondiente sobre protección de datos.

4. Cada órgano superior o directivo del Ministerio de Hacienda y Función Pública, así como cada organismo o entidad de derecho público vinculado o dependiente del Departamento a los que, conforme al artículo 1, les sea de aplicación la presente PSI, designará estos perfiles de acuerdo con su propia organización interna, sin que, de acuerdo con lo previsto en la disposición adicional primera de la presente Orden, implique, en ningún caso, un aumento de las actuales dotaciones ni de las retribuciones de dichos efectivos por ningún concepto.

Artículo 10. *Los Responsables del Sistema.*

1. El Responsable del Sistema es la persona cuya responsabilidad es desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida.

2. Cada órgano superior o directivo del Ministerio de Hacienda y Función Pública, así como cada organismo o entidad de derecho público vinculado o dependiente del Departamento a los que, conforme al artículo 1, les sea de aplicación la presente PSI, designará este perfil de acuerdo con su propia organización interna, sin que, de acuerdo con lo previsto en la disposición adicional primera de la presente Orden, implique, en ningún caso, un aumento de las actuales dotaciones ni de las retribuciones de dichos efectivos por ningún concepto.

Artículo 11. *El Delegado de Protección de Datos.*

El Delegado de Protección de Datos, designado en virtud de lo dispuesto en los apartados 1.s) y 2.e) del artículo 14 del Real Decreto 1113/2018, de 7 de septiembre, por el que se desarrolla la estructura orgánica básica del Ministerio de Hacienda, en virtud de lo establecido en el Reglamento General de Protección de Datos (Reglamento UE 2016/679) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, es único para todo el Departamento, sin perjuicio de la existencia de Delegados de Protección de Datos en los organismos públicos adscritos al Departamento y del nombramiento de coordinadores en todos los órganos superiores del Departamento y en la Intervención General de la Administración del Estado.

Artículo 12. *Los Responsables y Encargados de tratamiento de datos personales.*

1. El responsable de tratamiento es la persona física o jurídica, autoridad pública, servicio u otra entidad que, solo o junto con otros, determina los fines y medios del tratamiento y aplica las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con la normativa vigente en materia de protección de datos personales.

La identidad del responsable de tratamiento figura en el registro de las actividades de tratamiento efectuadas bajo su responsabilidad, de acuerdo con lo dispuesto en el artículo 30 del Reglamento General de Protección de Datos.

2. El encargado de tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que trata datos personales por cuenta del responsable del tratamiento.

cve: BOE-A-2021-13777
Verificable en https://www.boe.es

Artículo 13. *Grupos de trabajo.*

El CDSI podrá articular la creación de grupos de trabajo para la realización de actividades tales como: estudios, trabajos e informes, que se estimen convenientes.

Artículo 14. *Gestión de los riesgos.*

1. La gestión de riesgos debe realizarse de manera continua sobre los sistemas de información y contemplar un análisis de riesgos avanzado que evalúe los riesgos residuales y proponga tratamientos adecuados. Cuando el análisis de riesgos se aplique a tratamientos de datos personales, se tendrán en cuenta los riesgos posibles que afecten a los derechos y libertades de las personas físicas.
2. Cada órgano superior o directivo del Ministerio de Hacienda y Función Pública, así como cada organismo o entidad de derecho público vinculado o dependiente del Departamento a los que, conforme al artículo 1, les sea de aplicación la presente PSI, y siempre dentro de su ámbito de actuación y de sus competencias, se encargará de analizar y evaluar los riesgos de funcionamiento de los servicios a fin de establecer las correspondientes medidas preventivas.
3. Para la realización del análisis de riesgos se tendrán en cuenta las recomendaciones publicadas para el ámbito de la Administración Pública y en especial las guías elaboradas por el Centro Criptológico Nacional y la Agencia Española de Protección de Datos.

Artículo 15. *Estructura normativa.*

1. El cuerpo normativo sobre seguridad de la información es de obligado cumplimiento y se estructura en los siguientes niveles relacionados jerárquicamente:

a) Primer nivel normativo: constituido por la PSI y las directrices generales de seguridad aplicables a los órganos superiores o directivos del Ministerio de Hacienda y Función Pública a los que, conforme al artículo 1, sea de aplicación la presente PSI.
b) Segundo nivel normativo: constituido por las normas de seguridad desarrolladas por cada órgano superior o directivo del Ministerio de Hacienda y Función Pública, así como por cada organismo público dependiente del Departamento a los que, conforme al artículo 1, les sea de aplicación la presente PSI. Estas normas de seguridad deberán:

1.º Limitarse única y exclusivamente al ámbito específico de las competencias de cada uno de dichos órganos u organismos adscritos a la presente PSI. 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 gestionados directamente por dicho órgano u organismo.
2.º Cumplir estrictamente con lo indicado en el ENS, con la normativa vigente en materia de protección de datos personales y con el primer nivel normativo enunciado en el presente artículo.
3.º Ser aprobadas dentro del ámbito de cada uno de los citados órganos u organismos adscritos a la presente PSI.

c) Tercer nivel normativo: Procedimientos, guías e instrucciones técnicas. Son documentos que, cumpliendo con lo expuesto en la PSI, determinan las acciones o tareas a realizar en el desempeño de un proceso. Este tercer nivel normativo deberá:

1.º Limitarse única y exclusivamente al ámbito específico de las competencias de cada uno de dichos órganos u organismos adscritos a la presente PSI. 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 gestionados directamente por dicho órgano u organismo.

cve: BOE-A-2021-13777
Verificable en https://www.boe.es

2.º Cumplir estrictamente con lo indicado en el ENS, con la normativa vigente en materia de protección de datos personales y con el primer y segundo nivel normativos enunciados en el presente artículo.

3.º Ser aprobado dentro del ámbito de cada uno de los citados órganos u organismos adscritos a la presente PSI.

2. Además de la normativa enunciada con anterioridad, la estructura normativa podrá disponer, a criterio de cada uno de los órganos u organismos adscritos a la presente PSI, y siempre dentro del ámbito de sus competencias y responsabilidades, de otros documentos tales como: estándares de seguridad, buenas prácticas, informes técnicos, etc.

3. El personal de cada uno de los órganos, organismos o entidades adscritos a 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.

Artículo 16. *Protección de datos de carácter personal.*

1. 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 al riesgo, teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas. El 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.

Esta responsabilidad 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 de datos personales relacionada en el art. 3 de esta Orden y el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, 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 Esquema Nacional de Seguridad.

2. 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 delegado de protección de datos al realizar la preceptiva evaluación de impacto relativa a la protección de datos.

3. 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 17. *Formación y concienciación.*

1. Se desarrollarán actividades formativas específicas orientadas a la concienciación y formación de los empleados públicos del Departamento, así como a la difusión entre los empleados de la PSI y de su desarrollo normativo.

2. El Grupo de trabajo técnico de Seguridad de la Información y los Responsables de Seguridad se encargarán de promover las actividades de formación y concienciación en materia de seguridad, según lo indicado en el artículo 7, apartado 3, letra f), y en el artículo 8, apartado 3, letra f), de esta Orden.

cve: BOE-A-2021-13777
Verificable en https://www.boe.es

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

Las medidas descritas en esta orden no supondrán incremento del gasto, siendo atendidas con los medios personales, técnicos y presupuestarios asignados al Ministerio de Hacienda y Función Pública.

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

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

Disposición derogatoria única. *Derogación normativa.*

Quedan derogadas las disposiciones de igual o inferior rango en lo que se opongan a lo dispuesto en esta orden ministerial y, en particular, la Orden HAP/1953/2014, de 15 de octubre, por la que se aprueba la política de seguridad de la información en el ámbito de la administración electrónica del Ministerio de Hacienda y Administraciones Públicas.

Disposición final única. *Publicidad de la PSI y entrada en vigor.*

1. La presente Orden entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».
2. Esta Orden se publicará en las sedes electrónicas del Ministerio de Hacienda y Función Pública en cuyo ámbito sea de aplicación.

Madrid, 29 de julio de 2021.–La Ministra de Hacienda y Función Pública, María Jesús Montero Cuadrado.

cve: BOE-A-2021-13777
Verificable en https://www.boe.es