Orden ISM/1320/2024, de 18 de noviembre, por la que se aprueba la Política de Seguridad de la Información del Ministerio de Inclusión, Seguridad Social y Migraciones y se crea el Comité de Seguridad de los Sistemas de Información.

Ministerio de Inclusión, Seguridad Social y Migraciones
«BOE» núm. 283, de 23 de noviembre de 2024
Referencia: BOE-A-2024-24452

TEXTO CONSOLIDADO
Última modificación: sin modificaciones

El marco de relación entre la Administración Pública y la ciudadanía 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 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 su artículo 158.

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 la ciudadanía realice los trámites administrativos correspondientes con total seguridad y fiabilidad. Para ello, el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, 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. El fundamento jurídico de esta orden se encuentra en el artículo 12 del mismo, que establece que cada administración pública contará con una política de seguridad formalmente aprobada por el órgano competente, y, en el caso de la Administración General del Estado, cada ministerio contará con su política de seguridad, que aprobará la persona titular del departamento, lo que enlaza con los principios de necesidad, seguridad jurídica y transparencia.

El Real Decreto 829/2023, de 20 de noviembre, por el que se reestructuran los departamentos ministeriales, atribuye en su artículo 21 al Ministerio de Inclusión, Seguridad Social y Migraciones la propuesta y ejecución de la política del Gobierno en materia de Seguridad Social y clases pasivas, así como la elaboración y el desarrollo de la política del Gobierno en materia de extranjería, inmigración y emigración y de políticas de inclusión. Con posterioridad, el Real Decreto 1009/2023, de 5 de diciembre, por el que se establece la estructura orgánica básica de los departamentos ministeriales, estableció en su artículo 20 la estructura del Ministerio de Inclusión, Seguridad Social y Migraciones hasta el nivel orgánico de dirección general. Recientemente, se ha determinado la estructura orgánica básica de

este departamento ministerial por el Real Decreto 501/2024, de 21 de mayo, por el que se desarrolla la estructura orgánica básica del Ministerio de Inclusión, Seguridad Social y Migraciones, y se modifica el Real Decreto 1009/2023, de 5 de diciembre, por el que se establece la estructura orgánica básica de los departamentos ministeriales.

Esta Política de Seguridad de la Información (en adelante PSI) es el instrumento en que se apoya el Ministerio de Inclusión, Seguridad Social y Migraciones para alcanzar sus objetivos utilizando de forma segura los sistemas de información y las comunicaciones. La seguridad, concebida como proceso integral, comprende todos los elementos técnicos, humanos, materiales y organizativos relacionados con los sistemas de información y las comunicaciones y debe entenderse no como un producto sino como un proceso continuo de adaptación y mejora, que debe ser controlado, gestionado y monitorizado, implementando la cultura de la seguridad en el Ministerio.

La PSI constituye el marco de referencia orientado a facilitar la definición, gestión, administración e implementación de los mecanismos y procedimientos de seguridad establecidos en el Esquema Nacional de Seguridad. Identifica responsabilidades y establece principios y directrices para una protección adecuada y consistente de los servicios y activos de información gestionados por medio de las Tecnologías de la Información y de las Comunicaciones.

Del mismo modo, el Real Decreto 311/2022, de 3 de mayo, determina que la PSI debe 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 la normativa vigente en esta materia, prevaleciendo éstos en lo relativo a la protección de datos de carácter personal en caso de discrepancias.

En este sentido, la entrada en vigor del citado Reglamento Europeo (UE) 2016/679, y de la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales, plantea nuevos retos, así como la necesidad de dar un nuevo enfoque al tratamiento de datos de carácter personal. De este modo, para garantizar su adecuada implantación resulta necesario intensificar la labor de coordinación con el resto de las normas de obligatoria implantación en la organización, especialmente con el Esquema Nacional de Seguridad, buscando sinergias en el desarrollo de ambas. Para garantizar la coordinación en la implantación de estas normativas se deberá procurar que:

a) El cumplimiento del Esquema Nacional de Seguridad y la legislación de protección de datos estén alineados, apoyándose mutuamente en el caso de los sistemas de información que tratan datos de carácter personal.

b) Los planes de concienciación y formación que se definan contengan contenidos comunes en el ámbito de los tratamientos de datos de carácter personal.

c) Se establezca la correspondencia entre los tratamientos de datos de carácter personal y los sistemas de información identificados en el Esquema Nacional de Seguridad que incluyan datos de carácter personal, buscando unificar en una única declaración los requisitos y medidas de seguridad y de protección de los datos personales que son necesarios para cumplir con ambas normas.

d) Las auditorías de cumplimiento en particular y las revisiones de seguridad en general que incluyan controles de ambas normas, se efectúen de manera conjunta.

e) Se lleve a cabo una designación común de las responsabilidades, así como una relación con los organismos reguladores y de coordinación.

La PSI es de obligado cumplimiento para todo el personal que acceda a los sistemas de información o a la información del departamento, para sus órganos superiores y directivos que no tengan establecida su propia política de seguridad y para los aspectos no tratados en dichas políticas de seguridad particulares.

Esta orden se estructura en veinte artículos, tres disposiciones adicionales, dos disposiciones derogatorias y dos disposiciones finales. La disposición derogatoria primera deroga, en lo que afecta a las competencias del Ministerio de Inclusión, Seguridad Social y Migraciones, la Orden TIN/3016/2011, de 28 de octubre, por la que se crea el Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Ministerio de Trabajo e Inmigración, y la Orden comunicada de la Ministra de Empleo y Seguridad Social, de 30 de julio de 2012, por la que se aprueba la Política de Seguridad de los Sistemas de

Información del Ministerio de Empleo y Seguridad Social. También se deroga en la disposición derogatoria segunda la Orden ISM/254/2021, de 16 de marzo, por la que se crea y regula la Comisión Asesora de Estudios y se establece la regulación del Programa anual de Estudios del departamento, por tratarse de otra norma de naturaleza organizativa de acuerdo con las competencias de la Subsecretaría de Inclusión, Seguridad Social y Migraciones previstas en el Real Decreto 501/2024, de 21 de mayo.

La norma se ajusta a los principios de buena regulación contenidos en el artículo 129 de la Ley 39/2015, de 1 de octubre. En concreto, se adecúa a los principios de necesidad y eficacia puesto que, con la aprobación de la norma, se dota al departamento ministerial de un marco que garantiza la seguridad en la utilización de sus activos de información.

Asimismo, es también adecuada al principio de proporcionalidad, en cuanto se trata de una norma puramente organizativa que, en consecuencia, no restringe derechos ni libertades ni impone obligaciones.

Igualmente, a la vista de su objeto y contenido se considera cumplido el principio de eficiencia en la medida en que la norma prevé que los medios personales y financieros a utilizar son los ya existentes en el ministerio y, además, no se imponen cargas administrativas ni se afecta a las existentes.

Finalmente, se ajusta al principio de seguridad jurídica, pues resulta plenamente coherente con el resto del ordenamiento jurídico, y se da cumplimiento al principio de transparencia al quedar claramente delimitados los objetivos y fines perseguidos por esta orden ministerial.

En el proceso de su tramitación se han recabado informes de la Comisión Permanente de la Comisión Ministerial de Administración Digital del Ministerio de Inclusión, Seguridad Social y Migraciones, del delegado de protección de datos y de la Secretaría General Técnica del mismo ministerio, así como de la Agencia Española de Protección de Datos.

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

Artículo 1. *Objeto y ámbito de aplicación.*

1. El objeto de esta orden es la aprobación de la Política de Seguridad de la Información (en adelante PSI) en el ámbito del Ministerio de Inclusión, Seguridad Social y Migraciones, su marco organizativo y tecnológico, así como la creación del Comité de Seguridad de los Sistemas de Información y la regulación de su composición, funcionamiento y funciones.

2. La PSI será de obligado cumplimiento para todos los órganos superiores y directivos del Ministerio de Inclusión, Seguridad Social y Migraciones, con las excepciones que, en su caso, correspondan a la Secretaría de Estado de la Seguridad Social y Pensiones y a las entidades gestoras y servicios comunes de la Administración de la Seguridad Social adscritas a la misma.

3. Se podrán adscribir a la presente PSI aquellos organismos y entidades de derecho público vinculados o dependientes del Ministerio de Inclusión, Seguridad Social y Migraciones 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 Inclusión, Seguridad Social y Migraciones es el departamento encargado de la propuesta y ejecución de la política del Gobierno en materia de Seguridad Social y clases pasivas, así como de la elaboración y el desarrollo de la política del Gobierno en materia de extranjería, inmigración y emigración y de políticas de inclusión, de conformidad con lo establecido en el artículo 1 del Real Decreto 501/2024, de 21 de mayo, por el que se desarrolla la estructura orgánica básica del Ministerio de Inclusión, Seguridad Social y Migraciones, y se modifica el Real Decreto 1009/2023, de 5 de diciembre, por el que se establece la estructura orgánica básica de los departamentos ministeriales.

Artículo 3. *Marco normativo.*

El marco normativo en que se desarrollan las actividades del Ministerio de Inclusión, Seguridad Social y Migraciones en el ámbito de la prestación de los servicios electrónicos a la ciudadanía, sin perjuicio de la legislación específica, está integrado fundamentalmente por las siguientes disposiciones:

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

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

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

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

e) 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.

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

g) 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.

h) Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

i) Ley 12/1989, de 9 de mayo, de la Función Estadística Pública.

j) 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.

k) 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.

l) Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica.

m) 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.

n) 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.

o) Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

p) 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.

q) Orden ISM/11/2021, de 12 de enero, por la que se crea y regula la Sede Electrónica Central del Ministerio de Inclusión, Seguridad Social y Migraciones.

r) Orden TIN 1459/2010, de 28 de mayo, por la que se crea la Sede Electrónica de la Secretaría de Estado de la Seguridad Social.

s) Aquellas normas aplicables a la administración electrónica y seguridad de la información derivadas de las anteriores y publicadas en las sedes electrónicas dentro del ámbito de aplicación de la PSI del Ministerio.

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. Estos principios básicos, en su continuo fortalecimiento y revisión, se ajustarán en todo caso, de acuerdo con lo previsto en la disposición adicional segunda del Real Decreto 311/2022, de 3 de mayo, a las instrucciones técnicas de seguridad que publique la Secretaría de Estado de Función Pública del Ministerio para la Transformación Digital y de la

Función Pública, así como a las guías de seguridad de las tecnologías de la información y la comunicación (guías CCN-STIC) Complementando lo dispuesto en el capítulo II del Real Decreto 311/2022, de 3 de mayo, se establecen los siguientes principios básicos:

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 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 la persona responsable de la información, que determina los requisitos de seguridad de la información tratada; la persona responsable del servicio, que determina los requisitos de seguridad de los servicios prestados; la persona responsable del sistema, que tiene la responsabilidad de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad; y la persona responsable de la seguridad, que será distinta de la responsable del sistema, no debiendo existir dependencia jerárquica entre ambas, y que determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones. En los supuestos de tratamientos de datos personales se identificará además a la persona, organismo o unidad responsable de tratamientos y, en su caso, al encargado de tratamiento, de acuerdo con las definiciones del artículo 4.7 y 8 del Reglamento (UE) 2016/679.

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 de información, 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 los riesgos: el análisis y gestión de los riesgos será parte esencial del proceso de seguridad. La gestión de los riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción a estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerán 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. Además, las medidas de seguridad deberán garantizar el cumplimiento de lo previsto en el artículo 32 del Reglamento (UE) 2016/679, por lo que el responsable del tratamiento de datos personales, y en su caso, de los encargados del tratamiento, podrán adoptar todas aquellas medidas adicionales con el fin de garantizar la seguridad de los datos personales, en virtud de lo dispuesto en los artículos 24 y 25 del Reglamento (UE) 2016/679, en el artículo 28 de la Ley Orgánica 3/2018, de 5 de diciembre, y en el artículo 3 del Real Decreto 311/2022, de 3 de mayo.

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 con dichas competencias entre sus funciones.

g) Seguridad desde el diseño y por defecto: los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto. Además, con el fin de garantizar la resiliencia y la protección de los datos personales, se deben tener en cuenta las medidas de seguridad por defecto en base a los artículos 24 y 25 del Reglamento (UE) 2016/679, así como las medidas de seguridad orientadas al riesgo según el artículo 32 del Reglamento (UE) 2016/679.

h) Vigilancia continua: de forma que la evaluación permanente del estado de la seguridad de los activos permita medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración. En cuanto a la gestión de incidentes que afecten a datos

personales, se tendrán en cuenta las obligaciones específicas de notificación, comunicación y documentación especificadas en los artículos 33 y 34 del Reglamento (UE) 2016/679.

2. Principios particulares y responsabilidades específicas.

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 principios particulares y responsabilidades específicas:

a) Protección de datos de carácter personal: se adoptarán las medidas técnicas y organizativas destinadas a garantizar el nivel de seguridad exigido por la normativa vigente en relación con el tratamiento de los datos de carácter personal.

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. 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. Para proteger las redes del departamento, se analizará el tráfico cifrado de usuarios de forma automatizada. Se realizará la excepción en este análisis de las categorías de navegación relacionadas con datos sensibles especialmente protegidos de acuerdo con la normativa de protección de datos vigente, siempre que sea posible la discriminación.

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 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 con 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.

3. Sin perjuicio de lo establecido en los apartados 1 y 2, la presente PSI se establecerá en base a los principios básicos y se desarrollará aplicando los requisitos mínimos contemplados en el capítulo II y en el artículo 12.6 del Real Decreto 311/2022, de 3 de mayo.

4. Estos principios particulares, en su continuo fortalecimiento y revisión, se ajustarán en todo caso a las instrucciones técnicas de seguridad que publique la Secretaría de Estado de Función Pública del Ministerio para la Transformación Digital y de la Función Pública, así como a las guías CCN-STIC.

Artículo 5. *Estructura organizativa.*

La gestión de la seguridad en el Ministerio de Inclusión, Seguridad Social y Migraciones se apoya en la siguiente estructura organizativa:

a) La persona responsable del sistema global de información.
b) El Comité de Seguridad de los Sistemas de Información.
c) La persona responsable de sistemas de información.
d) La persona responsable de seguridad del Ministerio de Inclusión, Seguridad Social y Migraciones.
e) La persona responsable de la prestación del servicio.
f) El delegado o la delegada de protección de datos.

Artículo 6. *Persona responsable del sistema global de información.*

1. La persona titular de la Subsecretaría de Inclusión, Seguridad Social y Migraciones es la responsable del sistema global de información, y, además, es la responsable última del funcionamiento de los servicios.

El sistema global de información integra todos los sistemas de información de los órganos superiores y directivos y unidades dependientes del Ministerio de Inclusión, Seguridad Social y Migraciones, de los que son responsables las personas titulares de estos.

2. La persona responsable del sistema global de información tiene las siguientes funciones:

a) Hacer cumplir las disposiciones establecidas en el Esquema Nacional de Seguridad y en la Ley Orgánica 3/2018, de 5 de diciembre, cuando el sistema de información se encuentre dentro del ámbito de aplicación de estas y, en su caso, emitir directrices.
b) Resolver los conflictos que puedan surgir entre los distintos responsables de los sistemas de información, en el ejercicio de sus funciones, en los términos establecidos en el artículo 18.

Artículo 7. *Comité de Seguridad de los Sistemas de Información.*

1. Se crea el Comité de Seguridad de los Sistemas de Información (en adelante CSSI) que coordinará todas las actividades relacionadas con la seguridad de los sistemas de información en el ámbito del Ministerio de Inclusión, Seguridad Social y Migraciones. En los casos en los que el CSSI así lo decida, éste podrá asumir las funciones de responsable del sistema de información y de responsable de la prestación del servicio.

2. Como órgano colegiado de carácter transversal adscrito a la Subsecretaría de Inclusión, Seguridad Social y Migraciones, el CSSI tendrá la siguiente composición:

a) Presidencia: la persona titular de la Subsecretaría de Inclusión, Seguridad Social y Migraciones.
b) Vicepresidencia: la persona titular del Gabinete Técnico de la Subsecretaría.

c) Vocalías:

i) Una vocalía en representación de cada uno de los órganos superiores y directivos del Ministerio de Inclusión, Seguridad Social y Migraciones, con rango igual o superior a Dirección General o equivalente. La persona designada deberá tener un rango mínimo de subdirector general o asimilado.
ii) Una vocalía para la persona responsable de seguridad del Ministerio de Inclusión, Seguridad Social y Migraciones.
iii) Una vocalía para la persona titular de la Subdirección General de Tecnologías de la Información y Comunicaciones del Ministerio de Inclusión, Seguridad Social y Migraciones que, además, actuará como secretaria del CSSI.
iv) Una vocalía para la persona titular de la Gerencia de Informática de la Seguridad Social.
v) Una vocalía para el delegado o la delegada de protección de datos del Ministerio de Inclusión, Seguridad Social y Migraciones, que actuará como asesor con voz, pero sin voto, para garantizar su independencia en atención a la naturaleza de sus funciones de asistencia y apoyo.

3. En caso de vacante, ausencia o enfermedad, así como en los casos en que haya sido declarada su abstención o recusación y, en general, cuando concurra alguna causa justificada, se establece el siguiente régimen de suplencias de los miembros del CSSI:

a) La presidencia será sustituida por la vicepresidencia.
b) Las vocalías serán sustituidas por sus suplentes, que deberán ser personal funcionario pertenecientes al grupo A1, con nivel 28 o superior.

4. El CSSI tiene las siguientes funciones:

a) Definir y aprobar los planes estratégicos, líneas de actuación y objetivos en materia de seguridad del Ministerio de Inclusión, Seguridad Social y Migraciones, siempre alineados con la misión y objetivos de la organización.
b) Garantizar la divulgación de la PSI.
c) La aprobación y seguimiento de las normas y procedimientos en materia de seguridad que afecten transversalmente al Ministerio de Inclusión, Seguridad Social y Migraciones.
d) Establecer, cuando sea posible, criterios comunes de actuación en todos los órganos superiores y directivos de la organización para el cumplimiento de las normas o procedimientos en materia de seguridad de la información que sean de aplicación.
e) Revisar el estado global de la seguridad en cada uno de los órganos superiores y directivos dependientes del Ministerio de Inclusión, Seguridad Social y Migraciones.
f) Trasladar las directrices que sean establecidas por el CSSI a cada uno de los órganos superiores y directivos y garantizar su cumplimiento.
g) Actualizar y asignar las funciones y obligaciones de la PSI de cada uno de los responsables definidos en el artículo 2.
h) Promover líneas de trabajo para una adecuada concienciación y formación en materia de seguridad para el personal del Ministerio de Inclusión, Seguridad Social y Migraciones.
i) Ser informado, deliberar e intercambiar información con los órganos superiores y directivos del Ministerio de Inclusión, Seguridad Social y Migraciones que sean responsables de tratamientos con datos de carácter personal para tratar y asesorar sobre las medidas de seguridad técnica y las medidas de protección de la información aplicables en los sistemas y servicios que les afecten.

5. El CSSI se reunirá con carácter ordinario como mínimo tres veces al año y, con carácter extraordinario, cuando la presidencia lo considere necesario. Las sesiones se celebrarán de forma presencial o a distancia, lo que se especificará necesariamente en la convocatoria.
6. El CSSI podrá recabar del personal técnico, propio o externo, la información pertinente para la toma de sus decisiones. Asistirán en su caso en calidad de asesores con voz, pero sin voto.
7. La secretaría del CSSI levantará el acta de cada reunión del comité y realizará, junto con la persona responsable de seguridad del departamento, todos los trabajos previos necesarios apoyándose cuando lo requiera en las unidades y organismos del departamento.
8. En lo no previsto en esta orden, el funcionamiento del CSSI 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. *Persona responsable de sistemas de información.*

1. Las personas responsables de los sistemas de información garantizan, en sus respectivos ámbitos, la puesta en marcha, mantenimiento y actualización de las medidas pertinentes en materia de seguridad de los sistemas de información. Asimismo, determinan los requisitos de seguridad de la información tratada, de los tratamientos realizados sobre la misma y de los servicios electrónicos que se prestan, en sus respectivos ámbitos.
2. Se designan como responsables de sus sistemas de información a las personas titulares de todos los órganos superiores y directivos del Ministerio de Inclusión, Seguridad Social y Migraciones y a las personas titulares de todos los organismos adscritos y órganos dependientes de los órganos superiores y directivos del Ministerio de Inclusión, Seguridad Social y Migraciones para la información que tratan en el ejercicio de sus competencias, sin

perjuicio de que estos puedan delegar ciertas funciones en las direcciones y subdirecciones provinciales correspondientes.

3. Las personas responsables de los sistemas de información son responsables del tratamiento, responsables de la información y responsables de los servicios electrónicos en todos los sistemas de información que traten datos personales.

4. A las personas responsables de los sistemas de información les corresponden las siguientes funciones:

a) Garantizar que se gestiona el riesgo de seguridad de sus sistemas de información.

b) Definir los requisitos de seguridad de los sistemas de información de los que son responsables y, para cada uno de ellos, su nivel de riesgo residual aceptable.

c) Suspender el manejo de una determinada información o la prestación de un servicio si es informado de deficiencias graves de seguridad.

d) Adoptar las medidas necesarias para que el personal con acceso a sus sistemas de información conozca las normas de seguridad que debe aplicar.

e) Identificar y valorar la criticidad de la información que manejan y determinar en función de esta los requisitos de seguridad que es necesario cumplir para cada tipo de información.

f) Determinar el ciclo de vida de la información manejada y determinar los procedimientos de creación, tratamiento y destrucción de esta.

g) En cuanto a tratamientos con datos personales, deberán satisfacer los derechos de las personas titulares de los datos, registrar la condición que legitima el tratamiento, atender los derechos de información, acceso, rectificación, oposición, supresión («derecho al olvido»), limitación del tratamiento, portabilidad y de no ser objeto de decisiones individuales automatizadas y realizar la evaluación de impacto en la privacidad.

h) Comunicar al delegado o delegada de protección de datos correspondiente, con carácter previo a su uso, los nuevos tratamientos de alto riesgo con datos personales.

Artículo 9. *Persona responsable de la prestación del servicio.*

1. La persona responsable de la prestación del servicio tiene la obligación de implementar las medidas de seguridad sugeridas por la persona responsable de seguridad, que están incluidas en el plan director de seguridad.

2. Se designa como persona responsable de la prestación del servicio a la persona titular de la Subdirección General de Tecnologías de la Información y Comunicaciones, sin perjuicio de que pueda delegar ciertas funciones.

3. La persona responsable de la prestación del servicio tiene las siguientes funciones:

a) Implementar las medidas de seguridad que entren en su ámbito de actuación establecidas en el plan director de seguridad elaborado por la persona responsable de seguridad y aprobado por la persona responsable del sistema de información.

b) Observar el cumplimiento de las normas y procedimientos establecidos y aprobados por el CSSI en la administración y operativa habitual de los sistemas de información.

c) Supervisar y garantizar la gestión, configuración y actualización de los recursos que soportan el funcionamiento correcto de los sistemas de información y de la prestación de los servicios.

d) Colaborar en las auditorias llevadas a cabo por la persona responsable de seguridad, y aportar información completa y veraz sobre el estado de las medidas de seguridad implantadas que sean de su responsabilidad.

Artículo 10. *Persona responsable de seguridad.*

1. La persona responsable de seguridad es la encargada de determinar las decisiones para satisfacer los requisitos de seguridad de la información, los tratamientos y los servicios electrónicos.

2. La Subdirección General de Tecnologías de la Información y Comunicaciones designará a la persona responsable de seguridad preservando la debida independencia y sin perjuicio de que ésta pueda delegar ciertas funciones. Las personas titulares de todos los órganos superiores y directivos del Ministerio de Inclusión, Seguridad Social y Migraciones podrán nombrar su propio responsable de seguridad en su ámbito de competencia.

3. La persona responsable de seguridad tiene las siguientes funciones:

a) Determinar las decisiones necesarias para satisfacer los requisitos de seguridad de la información, de los tratamientos y de los servicios que hayan sido establecidos por sus respectivos responsables.

b) Realizar periódicamente un proceso de análisis de los riesgos de los sistemas de información que permita identificar los riesgos a los que éste se encuentra expuesto y las medidas para asegurar el nivel de riesgo residual aceptable aprobado para cada sistema de información.

c) Establecer el conjunto de proyectos y actuaciones que conformarán el plan director de seguridad que permitirá implantar las medidas de seguridad propuestas, y elevarlo al responsable global del sistema de información.

d) Realizar el seguimiento y control del estado de la seguridad del sistema de información y verificar que las medidas de seguridad definidas son adecuadas para la protección de la información y los servicios.

e) Realizar las auditorias periódicas que se determinen en cada sistema de información, incluyendo las revisiones relativas a protección de datos, para garantizar la correcta aplicación de las medidas de seguridad y el cumplimiento de las normas y procedimientos vigentes en la organización. El informe resultante de las mismas se enviará a las personas responsables de los sistemas de información y a las personas responsables de la prestación del servicio para subsanar las deficiencias encontradas.

f) Redactar, cuando sea necesario, las declaraciones de aplicabilidad de los sistemas de información respecto al Esquema Nacional de Seguridad.

g) Asistir al delegado o delegada de protección de datos del Ministerio de Inclusión, Seguridad Social y Migraciones y, en su caso, al delegado o delegada de protección de datos de la Secretaría de Estado de la Seguridad Social y Pensiones, en cuantas actuaciones relativas a la seguridad de los sistemas de información en las que sean requeridos.

h) Aprobar planes de formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad y elevarlos al CSSI para su incorporación en los planes de los organismos o unidades dependientes del Ministerio de Inclusión, Seguridad Social y Migraciones, así como establecer actuaciones disuasorias a favor de la seguridad.

Artículo 11. *Delegado o delegada de protección de datos.*

1. El delegado o la delegada de protección de datos, designado en virtud de lo dispuesto en el artículo 10.3.j) del Real Decreto 501/2024, de 21 de mayo, por el que se desarrolla la estructura orgánica básica del Ministerio de Inclusión, Seguridad Social y Migraciones, y se modifica el Real Decreto 1009/2023, de 5 de diciembre, por el que se establece la estructura orgánica básica de los departamentos ministeriales, en virtud de lo establecido en el Reglamento (UE) 2016/679 y en la Ley Orgánica 3/2018, de 5 de diciembre, es único para todo el departamento, sin perjuicio de la existencia del delegado o delegada de protección de datos de la Secretaría de Estado de la Seguridad Social y Pensiones.

2. En el ámbito de los tratamientos de datos personales, y sin perjuicio de las atribuciones establecidas en el Reglamento (UE) 2016/679 de forma exclusiva a los responsables y encargados de los tratamientos de datos personales, y de las atribuciones exclusivas de las personas responsables de la seguridad, el delegado o delegada de protección de datos ejercerá labores de asesoramiento y supervisión en el ámbito de la presente norma.

3. El delegado o delegada de protección de datos prestará asistencia y asesoramiento a las personas responsables del tratamiento a la hora de identificar los riesgos y adoptar medidas para la protección de los datos personales, y en cuanto a la supervisión de que las mismas se han adoptado y llevado a la práctica. En cualquier caso, las funciones ejecutivas de toma de las decisiones oportunas al respecto serán responsabilidad de los respectivos responsables del tratamiento.

4. El delegado o delegada de protección de datos ejercerá labores de asistencia y asesoramiento a las personas responsables del tratamiento de datos personales, a las personas responsables de la seguridad y a las personas responsables del sistema, en los

procesos de gestión de brechas de datos personales en el ámbito de la gestión general de incidentes de seguridad.

5. El delegado o delegada de protección de datos prestará asesoramiento a las personas responsables de la seguridad y a las personas responsables del sistema, en cuanto a la implantación de medidas de seguridad que tengan un objeto distinto que la protección de datos, en la medida en que impliquen un tratamiento adicional de datos personales, tal y como dispone el artículo 24 del Real Decreto 311/2022, de 3 de mayo.

6. El delegado o delegada de protección de datos participará en el CSSI en materia de protección de datos personales en el compartido objetivo de procurar:

a) Alinear las respectivas normativas de cumplimiento, así como la definición e implantación de medidas de seguridad.

b) Impulsar y/o coordinar auditorías y revisiones del estado de cumplimiento de los requisitos y principios de la legislación aplicable.

c) Diseñar planes de formación y concienciación conjuntos con los de seguridad de la información.

Artículo 12. *Los responsables y los 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 (UE) 2016/679.

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.

Artículo 13. *Gestión de los riesgos.*

1. Se realizará de forma periódica un proceso de análisis de riesgos sobre los sistemas de información, conforme a los principios de gestión de la seguridad basada en los riesgos y reevaluación periódica establecidos en el Esquema Nacional de Seguridad.

2. La persona responsable de seguridad es la encargada de realizar el análisis de riesgos de los sistemas de información, garantizando que el mismo se lleva a cabo de forma correcta y completa, y comunicando los resultados a las personas responsables de los sistemas de información. Además, realizará el seguimiento y control de las acciones a realizar como consecuencia de los resultados del análisis de riesgos.

3. La persona responsable del sistema de información es quien gestiona y asume los riesgos sobre sus sistemas de información.

Artículo 14. *Estructura de la documentación de seguridad del Ministerio de Inclusión, Seguridad Social y Migraciones.*

1. La presente PSI debe ser desarrollada en diferente documentación de seguridad que detalle y concrete los requisitos de seguridad de la información y los servicios, las tareas necesarias para garantizar su cumplimiento y las responsabilidades de todo el personal implicado en las mismas.

2. En el Ministerio de Inclusión, Seguridad Social y Migraciones esta documentación de seguridad se estructura en los siguientes niveles:

a) La PSI: documento con el conjunto de directrices que rigen la forma en que el Ministerio de Inclusión, Seguridad Social y Migraciones gestiona y protege la información que trata y los servicios que presta.

b) Las normas de seguridad: conjunto de documentos que determinan los objetivos de seguridad y directrices generales en cada ámbito concreto y que establecen las responsabilidades del personal implicado. Deben ser globales, concisas y definir puntos de contacto para su interpretación correcta. Serán aprobadas por el CSSI y serán de obligado cumplimiento en toda la organización.

c) Los procedimientos de seguridad: conjunto de documentos que describen explícitamente y paso a paso cómo realizar determinadas tareas para cumplir lo estipulado en las normas de seguridad. Cada procedimiento debe detallar al menos en qué condiciones debe aplicarse, quienes deben llevarla a cabo y qué hacer en cada momento. Serán de obligado cumplimiento en su ámbito correspondiente, pero no requieren aprobación del CSSI.

d) Las guías de seguridad: documentación que incluye recomendaciones de actuación para mejorar la eficacia y eficiencia de los procedimientos de seguridad, suministra información adicional de apoyo y propone buenas prácticas. No se consideran de obligado cumplimiento ni requieren aprobación del CSSI, proporcionándose a título meramente informativo.

Artículo 15. *Protección de datos de carácter personal.*

1. Se aplicarán a los datos de carácter personal que sean objeto de tratamiento por parte del Ministerio de Inclusión, Seguridad Social y Migraciones, las medidas técnicas y organizativas, y de seguridad apropiadas derivadas del análisis de riesgos, así como de la evaluación de impacto relativa a la protección de datos, que se detalla en el Reglamento (UE) 2016/679 y en la Ley Orgánica 3/2018, de 5 de diciembre.

Además, se aplicarán las medidas correspondientes al anexo II del Real Decreto 311/2022, de 3 de mayo. En el caso de que el análisis de riesgos determine medidas agravadas respecto a la normativa recogida en las medidas del citado anexo, las medidas derivadas del análisis de riesgos serán las que se implementarán en la protección de datos de carácter personal.

En particular, se tendrá en cuenta el artículo 32 del Reglamento (UE) 2016/679, en cuanto a la exigencia de una identificación de riesgos específicos para los derechos y libertades de las personas en relación a los tratamientos de datos personales, que debe ser previo al análisis de riesgos de los sistemas donde se implementen dichos tratamientos, de forma que el nivel de seguridad sea adecuado al riesgo que los tratamientos de datos personales suponen para los derechos y libertades de las personas.

2. Los servicios de ciberseguridad y administración de sistemas, dependientes de los respectivos responsables de los sistemas, podrán implementar tratamientos de datos personales como consecuencia de la implantación de medidas de seguridad que tengan un objeto distinto que la protección de los datos personales, en base a lo dispuesto en el artículo 24 del Real Decreto 311/2022, de 3 de mayo, y teniendo en cuenta, entre otros, los principios de limitación de finalidad; prohibición del tratamiento de los datos personales para fines distintos; el principio de minimización de datos, identificando los datos personales o las categorías de datos personales que pudieran ser tratados; o del principio de limitación del plazo de conservación, identificando los plazos máximos de conservación de los datos personales.

Artículo 16. *Responsabilidad del personal.*

Todo el personal que forme parte del Ministerio de Inclusión, Seguridad Social y Migraciones o que colabore con él en el ejercicio de sus funciones, deberá conocer y aplicar en su ámbito de actuación esta PSI, así como las normas y procedimientos de seguridad de cada sistema de información al que tenga acceso. Estas normas y procedimientos les serán proporcionadas por la persona responsable de cada sistema de información.

Artículo 17. *Relación con otras administraciones públicas.*

Cuando el Ministerio de Inclusión, Seguridad Social y Migraciones preste servicios o ceda información a otras administraciones públicas, les hará partícipes de esta PSI y de las normas de seguridad que apliquen. Las administraciones públicas receptoras quedarán sujetas a las obligaciones establecidas en ellas, debiendo desarrollar sus propios procedimientos para satisfacerlas.

Artículo 18. *Resolución de conflictos.*

En caso de conflicto entre los diferentes responsables, éste será resuelto por el superior jerárquico de los mismos. En defecto de lo anterior, prevalecerá la decisión de la persona responsable del sistema global de información.

Artículo 19. *Formación y concienciación.*

1. El CSSI, en coordinación con la Subdirección General de Recursos Humanos e Inspección de Servicios del Ministerio de Inclusión, Seguridad Social y Migraciones, desarrollará actividades específicas orientadas a la formación y concienciación de su personal en materia de seguridad de la información, así como a la difusión de la presente PSI y su desarrollo normativo, en particular entre el personal de nueva incorporación. A estos efectos, los planes de formación del Ministerio de Inclusión, Seguridad Social y Migraciones incluirán actividades formativas específicas sobre esta materia.

2. El CSSI promoverá una cultura de seguridad de la información alineada con la PSI entre aquellas organizaciones y usuarios externos que tengan acceso por acuerdo o convenio a sus sistemas de información.

Artículo 20. *Actualización y revisión periódica.*

1. La PSI deberá mantenerse actualizada para adecuarla al progreso de los servicios de la administración electrónica, a la evolución tecnológica y al desarrollo de la sociedad de la información, así como a los estándares internacionales de seguridad.

2. Las propuestas de revisión de la PSI se elaborarán por el CSSI que, con tal objetivo, revisará regularmente la oportunidad, idoneidad, completitud y precisión de lo establecido en la misma.

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

Las medidas incluidas en esta orden no supondrán incremento del gasto, siendo atendidas con los medios personales, técnicos y presupuestarios asignados al Ministerio de Inclusión, Seguridad Social y Migraciones.

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

Todos los órganos superiores y directivos del Ministerio de Inclusión, Seguridad Social y Migraciones y sus organismos adscritos y órganos dependientes colaborarán en las actuaciones de implementación de la PSI aprobada por esta orden.

Disposición adicional tercera. *Vigencia de políticas y normas de seguridad.*

Todas las políticas y normas de seguridad anteriores a la publicación de esta PSI permanecerán vigentes mientras no se acuerde por el CSSI la publicación de una nueva que la sustituya.

Cualquier actuación posterior a la publicación de esta PSI relativo a políticas o normas de seguridad deberán ser informados al CSSI con el objetivo de mantener unas líneas estratégicas de gestión de la seguridad de la información y de la protección de datos personales coherentes y complementarias.

Disposición derogatoria primera. *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, en lo que afecta a las competencias del Ministerio de Inclusión, Seguridad Social y Migraciones, las siguientes:

a) Orden TIN/3016/2011, de 28 de octubre, por la que se crea el Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Ministerio de Trabajo e Inmigración.

b) Orden comunicada de la Ministra de Empleo y Seguridad Social, de 30 de julio de 2012, por la que se aprueba la Política de Seguridad de los Sistemas de Información del Ministerio de Empleo y Seguridad Social.

Disposición derogatoria segunda. *Derogación normativa.*

Queda derogada la Orden ISM/254/2021, de 16 de marzo, por la que se crea y regula la Comisión Asesora de Estudios y se establece la regulación del Programa anual de Estudios del departamento.

Disposición final primera. *Instrucciones de aplicación.*

La persona titular de la Subsecretaría de Inclusión, Seguridad Social y Migraciones podrá dictar las instrucciones necesarias para el adecuado cumplimiento de esta orden.

Disposición final segunda. *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 la sede electrónica del Ministerio de Inclusión, Seguridad Social y Migraciones y en todas aquellas sedes electrónicas en cuyo ámbito sea de aplicación.

Madrid, 18 de noviembre de 2024.–La Ministra de Inclusión, Seguridad Social y Migraciones, Elma Saiz Delgado.