III. OTRAS DISPOSICIONES

MINISTERIO DE DERECHOS SOCIALES Y AGENDA 2030

17235 *Orden DSA/1142/2021, de 8 de octubre, por la que se aprueba la Política de Seguridad de la Información en el ámbito de la administración electrónica del Ministerio de Derechos Sociales y Agenda 2030.*

El desarrollo de la Administración Electrónica implica el tratamiento automatizado de grandes cantidades de información por los sistemas de tecnologías de la información y de las comunicaciones, que está sometida a diferentes tipos de amenazas y vulnerabilidades.

En el contexto de la Administración Electrónica, se entiende por seguridad de la información la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes y acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad, confidencialidad y trazabilidad de los datos almacenados o transmitidos y de los servicios que dichas redes o sistemas ofrecen, o a través de los cuales se realiza el acceso.

La Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece que las Administraciones Públicas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos. Dichos medios deben asegurar la interoperabilidad y seguridad de los sistemas y soluciones adoptadas, garantizarán la protección de los datos de carácter personal y facilitarán preferentemente la prestación conjunta de servicios a los interesados. En este sentido, el artículo 156 de la citada Ley 40/2015, de 1 de octubre, regula el Esquema Nacional de Seguridad.

Por su parte, la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, recoge en su artículo 13 sobre 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.

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, tiene por objeto determinar la política de seguridad en la utilización de medios electrónicos en su ámbito de aplicación, sus principios básicos y los requisitos mínimos que permitan una protección adecuada de la información.

El artículo 11 del citado Real Decreto 3/2010, de 8 de enero, exige que todos los órganos superiores de las Administraciones Públicas dispongan formalmente de su política de seguridad, que se aprobará por el titular del órgano superior correspondiente. Esta política de seguridad se establecerá con base en los principios básicos recogidos en el capítulo II de la propia norma: seguridad integral, gestión de riesgos, prevención, reacción y recuperación, líneas de defensa, reevaluación periódica y función diferenciada, y desarrollará una serie de requisitos mínimos consignados en el mencionado artículo 11.1.

Asimismo, su exigencia se puede deducir en: el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos); la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales; el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

cve: BOE-A-2021-17235
Verificable en https://www.boe.es

La presente orden, por tanto, tiene la finalidad de aprobar la Política de Seguridad de la Información del Ministerio de Derechos Sociales y Agenda 2030, así como establecer la estructura organizativa para definirla, implantarla y gestionarla.

Esta orden cumple con los principios de necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia y eficiencia recogidos en el artículo 129 de la Ley 39/2015, de 1 de octubre. Así, atiende a la necesidad de aprobar la Política de Seguridad de la Información del Ministerio de Derechos Sociales y Agenda 2030, y da cumplimiento al mandato contenido en el artículo 11 del Real Decreto 3/2010, de 8 de enero. Además, es eficaz y proporcionada en el cumplimiento de este propósito sin afectar en forma alguna a los derechos y deberes de la ciudadanía. También contribuye a dotar de mayor seguridad jurídica a la organización y funcionamiento de la Administración General del Estado, en lo que se refiere al Ministerio de Derechos Sociales y Agenda 2030. Cumple también con el principio de transparencia, ya que identifica claramente su propósito y, aunque la tratarse de una norma puramente organizativa su tramitación no ha requerido de la consulta pública previa y de los trámites de audiencia e información pública, junto con su memoria donde se ofrece una explicación completa de su contenido, la misma se ha encontrado accesible a la ciudadanía durante dicha tramitación. Finalmente, es también adecuada al principio de eficiencia, ya que no impone cargas administrativas.

Durante su tramitación, se han recabado los informes de la Comisión Ministerial de Administración Digital del Ministerio de Derechos Sociales y Agenda 2030 y de la Agencia Española de Protección de Datos.

En virtud de lo anterior, con la aprobación previa de la Ministra de Hacienda y Función Pública, dispongo:

Artículo 1. *Objeto y ámbito de aplicación.*

1. El objeto de la presente orden es la aprobación de la Política de Seguridad de la Información (en adelante, PSI) en el ámbito de la Administración Electrónica del Ministerio de Derechos Sociales y Agenda 2030, así como el establecimiento del marco organizativo y tecnológico de la misma.

2. La PSI será de obligado cumplimiento por todos los órganos y unidades del Departamento incluidos los organismos dependientes o adscritos al mismo que no tengan establecida su propia política de seguridad, en relación a todos los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias.

3. La PSI deberá ser cumplida, igualmente, por todo el personal destinado en dichos órganos y unidades, así como por aquellas personas que, aunque no estén destinadas en los mismos, tengan acceso a dichos datos, informaciones o servicios, con independencia de cuál sea su destino, adscripción o relación con el mismo.

Artículo 2. *Misión del Departamento.*

1. Corresponde al Ministerio de Derechos Sociales y Agenda 2030, según lo establecido en Real Decreto 452/2020, de 10 de marzo, por el que se desarrolla la estructura orgánica básica del Ministerio de Derechos Sociales y Agenda 2030, 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, la propuesta y ejecución de la política del Gobierno en materia de derechos sociales y bienestar social, de familia y de su diversidad, de protección del menor, de cohesión social y de atención a las personas dependientes o con discapacidad, de adolescencia y juventud, así como de protección de los animales.

2. Igualmente corresponde al Ministerio de Derechos Sociales y Agenda 2030 la propuesta y ejecución de la política del Gobierno en materia de impulso, seguimiento y

cve: BOE-A-2021-17235
Verificable en https://www.boe.es

cooperación para la implementación de la Agenda 2030 y el cumplimiento de los Objetivos de Desarrollo Sostenible.

Artículo 3. *Marco normativo.*

El marco normativo en que se desarrollan las actividades del Ministerio de Derechos Sociales y Agenda 2030, en el ámbito de la prestación de los servicios electrónicos a los ciudadanos, sin perjuicio de la legislación específica, se compone de:

1. Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
2. Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
3. 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.
4. 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.
5. 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.
6. 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).
7. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
8. Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.
9. La legislación sectorial reguladora de la actuación de los órganos superiores y directivos del Ministerio de Derechos Sociales y Agenda 2030, así como el Real Decreto 452/2020, de 10 de marzo, por el que se desarrolla la estructura orgánica básica del Ministerio de Derechos Sociales y Agenda 2030, 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.
10. Orden DSA/1082/2020, de 13 de noviembre, por la que se crea y regula el funcionamiento de la Comisión Ministerial de Administración Digital
11. Resolución de 24 de febrero de 2010, del Instituto de Mayores y Servicios Sociales, por la que se crea y regula la sede electrónica y el registro electrónico del Instituto de Mayores y Servicios Sociales.
12. 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.
13. Texto refundido de la Ley de Propiedad Intelectual, aprobado por Real Decreto Legislativo 1/1996, de 12 de abril, y su normativa de desarrollo.
14. 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.
15. 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.

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.

cve: BOE-A-2021-17235
Verificable en https://www.boe.es

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 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 se identificará además 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 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

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: de acuerdo a lo establecido en los artículos 24, 25 y 32 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en el artículo 28 de la Ley Orgánica 3/2018, de 5 de diciembre, así como en el artículo 6 del Real Decreto 3/2010, de 8 de enero, 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 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. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales

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, dedicado y diferenciado.

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, debiendo tener en cuenta la protección de datos personales en los supuestos en que aplique.

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

cve: BOE-A-2021-17235
Verificable en https://www.boe.es

inspiran las actuaciones del Departamento en dicha materia. Se establecen los siguientes:

a) Protección de datos personales: se adoptarán las medidas técnicas y organizativas destinadas a garantizar una adecuada protección de los datos. 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 Ley Orgánica 3/2018, de 5 de diciembre, dichas medidas deberán ser apropiadas en función del análisis de riesgos, así como de una evaluación de impacto relativa a la protección de datos cuando sea probable que un tratamiento, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas.

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.

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 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.

k) Derechos y deberes de los empleados públicos: Los empleados públicos que prestan servicio al Departamento tienen el derecho y el deber de conocer y aplicar la presente PSI y todas las directrices generales, normas y procedimientos de seguridad de la información que puedan afectar a sus funciones, así como de participar en acciones de difusión y formación orientadas a mejorar el estado de la seguridad de la información.

cve: BOE-A-2021-17235
Verificable en https://www.boe.es

3. Aplicabilidad de los principios y requisitos mínimos marcados en el Esquema Nacional de Seguridad.

Sin perjuicio de lo establecido en los apartados 1 y 2, la presente PSI se establecerá asimismo en base a los principios básicos y se desarrollará aplicando los requisitos mínimos contemplados en los artículos 4 y 11 del Real Decreto 3/2010, de 8 de enero.

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 Derechos Sociales y Agenda 2030 está compuesta por los siguientes agentes:

1. La Comisión Ministerial de Administración Digital.
2. El Responsable de Seguridad.
3. Los Responsables de la Información.
4. Los Responsables del Servicio.
5. Los Responsables del Sistema.
6. Los Delegados de Protección de Datos.

Artículo 6. *La Comisión Ministerial de Administración Digital.*

1. La Comisión Ministerial de Administración Digital, en adelante CMAD, es el órgano colegiado de ámbito departamental responsable del impulso y coordinación interna en materia de Administración Digital, según establece el artículo 1.2 de la Orden DSA/1082/2020, de 13 de noviembre.

2. La CMAD será la encargada de realizar las siguientes funciones:

a) Elaborar las propuestas de modificación y actualización permanente de la PSI.

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

c) Aprobar las normas de desarrollo de la PSI de segundo nivel, según lo previsto en el artículo 14.

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

e) Aprobar el Plan de Auditoría y el Plan de Formación propuestos por el Responsable de Seguridad.

f) Resolver los posibles conflictos que puedan derivarse del establecimiento de la estructura organizativa de seguridad, así como aquellos conflictos de competencia que pudieran aparecer entre los diferentes centros directivos en materia de seguridad de la información, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

g) Ordenar la realización de las auditorías o autoevaluaciones de seguridad y recibir información de los resultados de las mismas.

h) Proveer los recursos y medios necesarios para asegurar la concienciación y formación en materia de seguridad de la información de todo el personal afectado por esta orden.

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

j) Definir, dentro del marco establecido por la presente orden, la asignación de roles y los criterios para alcanzar las garantías que estime pertinentes en lo relativo a la segregación de tareas.

k) Apoyar la coordinación, cooperación y colaboración con otras Administraciones Públicas en materia de seguridad de la información a través de los órganos que se creen al respecto en las Administraciones Públicas.

l) Compartir experiencias de éxito en materia de seguridad entre sus miembros para velar por el cumplimiento de la PSI y su normativa de desarrollo.

cve: BOE-A-2021-17235
Verificable en https://www.boe.es

m) Informar sobre el estado de las principales variables de seguridad en los sistemas de información al Comité de Seguridad de la Información de las Administraciones Públicas para la elaboración de un perfil general del estado de seguridad de las mismas.

3. La Comisión podrá recabar de personal técnico, propio o externo, la información pertinente para la toma de sus decisiones.

4. La CMAD se reunirá con carácter ordinario al menos una vez al año y con carácter extraordinario cuando lo decida su Presidente.

Artículo 7. *Responsable de Seguridad.*

1. Conforme al artículo 10 del Real Decreto 3/2010, de 8 de enero, el Responsable de Seguridad es quien determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

2. Las funciones del Responsable de Seguridad se ejercerán por el Grupo Técnico de Seguridad de la Información (en adelante GTSI), órgano colegiado que se adscribe a la Subsecretaría, y que estará compuesto por los siguientes miembros:

a) Presidente: La persona titular de la Dirección de la División de Tecnologías de la Información y Comunicaciones. Tendrá voto de calidad en la toma de decisiones del grupo. En caso de ausencia, vacante o enfermedad será sustituido por el Vicepresidente.

b) Vicepresidente. La persona titular de la Coordinación de Área de la División de Tecnologías de la Información.

c) Vocales: La persona titular de la Jefatura de Área de Infraestructuras de la División de Tecnologías de la Información y un representante de cada uno de los organismos públicos adscritos a la presente política de seguridad, en el ámbito del Ministerio de Derechos Sociales y Agenda 2030. Los vocales representantes de los organismos públicos, así como sus sustitutos, serán designados por el titular de la Dirección del organismo público al que representen, adscrito a la presente PSI. El sustituto de la persona titular de la Jefatura de Área de Infraestructuras de la División de Tecnologías de la Información será designado por la persona titular de dicha División.

d) Secretario: La persona titular de la Jefatura de Área de Infraestructuras de la División de Tecnologías de la Información, que tendrá voz y voto y que, sin perjuicio del resto de funciones que le corresponden, ejecutará las decisiones del grupo, convocará sus reuniones y preparará los temas a tratar.

3. Serán funciones del Responsable de Seguridad las siguientes:

a) Promover y mantener la seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información.

b) Elaborar la normativa de seguridad de segundo nivel definida en el artículo 14 y proponer su aprobación al Pleno de la Comisión.

c) Velar e impulsar el cumplimiento del cuerpo normativo definido en el artículo 14.

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

e) Verificar que las medidas de seguridad son adecuadas para la protección de la información y los servicios.

f) Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución. Coordinar la comunicación con el Centro Criptológico Nacional en la utilización de servicios de respuesta a incidentes de seguridad.

g) Elaborar informes periódicos de seguridad que incluyan los incidentes más relevantes de cada período.

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

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

j) Aprobar la declaración de aplicabilidad, que comprende la relación de medidas de seguridad seleccionadas para un sistema.

cve: BOE-A-2021-17235
Verificable en https://www.boe.es

k) Realizar los preceptivos análisis de riesgos y mantenerlos actualizados según la legislación vigente.

l) Promover auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información, y analizar los informes de auditoría, elaborando las conclusiones a presentar a los Responsables del Servicio y los Responsables de la Información para que adopten las medidas correctoras adecuadas bajo su responsabilidad.

m) Realizar las tareas de coordinación y comunicación con los Responsables de Seguridad de los demás departamentos ministeriales.

n) Cualesquiera otras funciones que el Real Decreto 3/2010, de 8 de enero, asigne a los Responsables de Seguridad.

4. Cuando la complejidad, distribución, separación física de sus elementos o número de usuarios de los sistemas de información lo justifiquen, el GTSI podrá designar los Responsables de Seguridad delegados que considere necesarios, que tendrán dependencia funcional directa de aquél y serán responsables en su ámbito de todas aquellas acciones que les delegue el mismo.

5. A las reuniones del GTSI, podrán acudir representantes designados por los Delegados de Protección de Datos del Departamento y de los organismos públicos dependientes, adscritos a la presente PSI. También podrán ser invitados puntualmente los Responsables de los Tratamientos de Datos Personales en el ámbito del Departamento y de los organismos públicos adscritos. Puntualmente se podrá invitar a personal técnico propio o externo a las reuniones.

6. En el seno del GTSI, podrán crearse grupos de trabajo cuya función será la de apoyarlo en el ejercicio de sus funciones. Los grupos de trabajo tendrán la composición que, en cada caso, determine el GTSI.

7. El GTSI se reunirá con carácter ordinario con una periodicidad trimestral y con carácter extraordinario, cuando lo decida su Presidente. En cuanto a su funcionamiento, se regirá, en todo lo no previsto en la presente orden, por lo dispuesto en el capítulo II, sección 3.ª del título preliminar de la Ley 40/2015, de 1 de octubre.

Artículo 8. *Los Responsables de la Información.*

1. Conforme a los artículos 10 y 44 del Real Decreto 3/2010, de 8 de enero, el Responsable de la Información es la persona u órgano corporativo que tiene la potestad de establecer los requisitos de la información en materia de seguridad o, en terminología del Esquema Nacional de Seguridad, la potestad de determinar los niveles de seguridad de la información. Si estos servicios incluyen datos de carácter personal, además deberán tenerse en cuenta las medidas de seguridad que corresponda implantar atendidos los riesgos generados por el tratamiento de acuerdo a lo exigido por el citato Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

2. Serán funciones del Responsable de la Información, dentro de su ámbito 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 los Responsables del Servicio y contando con la participación del Responsable de la Seguridad, de realizar los preceptivos análisis de riesgos y seleccionar las salvaguardas que se han de implantar.

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

d) Para la determinación de los niveles de seguridad de la información, el Responsable de la Información solicitará informe del Responsable de la Seguridad.

cve: BOE-A-2021-17235
Verificable en https://www.boe.es

3. Los órganos superiores o directivos del Ministerio de Derechos Sociales y Agenda 2030, así como los organismos dependientes o adscritos al mismo a los que, conforme al artículo 1, sea de aplicación la presente PSI, designarán estos responsables de acuerdo con su propia organización interna, sin que implique, en ningún caso, un aumento de las actuales dotaciones ni de las retribuciones de dichos efectivos por ningún concepto. Se comunicarán los nombramientos al Responsable de Seguridad.

Artículo 9. *Los Responsables del Servicio.*

1. Conforme al artículo 10 del Real Decreto 3/2010, de 8 de enero, el Responsable del Servicio es la persona u órgano corporativo que tiene la potestad de establecer los requisitos del servicio en materia de seguridad. Es el encargado de determinar los niveles de seguridad del servicio en cada dimensión de seguridad, dentro del marco establecido en el anexo I del citado real decreto. Si estos servicios incluyen datos de carácter personal, además deberán tenerse en cuenta las medidas de seguridad que corresponda implantar atendidos los riesgos generados por el tratamiento de acuerdo a lo exigido por el citato Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

2. Los órganos superiores o directivos del Ministerio de Derechos Sociales y Agenda 2030, así como los organismos dependientes o adscritos al mismo a los que, conforme al artículo 1, sea de aplicación la presente PSI, designarán estos responsables de acuerdo con su propia organización interna, sin que implique, en ningún caso, un aumento de las actuales dotaciones ni de las retribuciones de dichos efectivos por ningún concepto.

Se comunicarán los nombramientos al Responsable de Seguridad.

Artículo 10. *Los Responsables del Sistema.*

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

2. Cada órgano superior o directivo del Ministerio de Derechos Sociales y Agenda 2030, así como cada organismo público 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, implique, en ningún caso, un aumento de las actuales dotaciones ni de las retribuciones de dichos efectivos por ningún concepto. Se comunicarán los nombramientos al Responsable de Seguridad.

3. Son funciones del Responsable del Sistema:

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

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

c) Posibilidad de acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los Responsables de la Información afectada, del Servicio afectado y el Responsable de la Seguridad, antes de ser ejecutada.

d) Para las demás funciones que por su naturaleza así lo requieran, se coordinará con la Secretaría General Técnica, especialmente a los efectos de eliminación de la información, de transferencia al archivo electrónico único y de cuantas otras actuaciones estén comprendidas en el marco del Sistema de Archivos del Ministerio de Derechos Sociales y Agenda 2030.

cve: BOE-A-2021-17235
Verificable en https://www.boe.es

Artículo 11. *Resolución de conflictos.*

1. En caso de conflicto entre los diferentes responsables, éste será resuelto por el superior jerárquico de los mismos. En su defecto, será la Comisión quien resuelva.
2. En la resolución de estos conflictos, prevalecerán las mayores exigencias derivadas de la protección de datos de carácter personal.

Artículo 12. *Obligaciones del personal.*

1. Todo el personal que presta servicios en el Ministerio de Derechos Sociales y Agenda 2030 y sus organismos adscritos, tienen la obligación de conocer y cumplir esta PSI y la normativa de seguridad derivada, siendo responsabilidad de la CMAD disponer los medios necesarios para que la información llegue a los afectados.
2. Todo el personal que se incorpore al Ministerio de Derechos Sociales y Agenda 2030 o vaya a tener acceso a alguno de sus sistemas de información o la información gestionada por ellos deberá ser informado y deberá cumplir la PSI y la normativa de seguridad derivada.
3. El incumplimiento manifiesto de la PSI o la normativa de seguridad derivada podrá acarrear el inicio de las medidas disciplinarias oportunas y, en su caso, las responsabilidades contractuales y legales correspondientes.

Artículo 13. *Los Delegados de Protección de Datos.*

1. El Delegado de Protección de Datos ejerce 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 capítulo III del título V de la Ley Orgánica 3/2018, de 5 de diciembre. Tendrá en todo caso acceso al registro de las actividades de tratamiento de datos personales al que se refiere el artículo 30 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

La actuación de los Delegados de Protección de Datos se regirá por el principio de independencia, por lo que no recibirán ninguna instrucción en lo que respecta al desempeño de sus funciones. Podrán estar asistidos por grupos de trabajo integrados por representantes de las unidades administrativas de su ámbito de actuación.

2. La designación de los Delegados de Protección de Datos del Ministerio de Derechos Sociales y Agenda 2030 y de los organismos dependientes o adscritos al mismo a los que, conforme al artículo 1, les sea de aplicación la presente PSI, se efectuará de conformidad con el artículo 37 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y el artículo 34 de la Ley Orgánica 3/2018, de 5 de diciembre. En consecuencia, serán designados atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones que tienen encomendadas. Se comunicarán los nombramientos al Responsable de Seguridad.

Artículo 14. *Estructura normativa.*

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

a) Primer nivel normativo: PSI y directrices. Está constituido por la PSI y las directrices fundamentales de seguridad aplicables a los órganos superiores o directivos del Ministerio de Derechos Sociales y Agenda 2030 a los que, conforme al artículo 1, sea de aplicación la presente PSI.

b) Segundo nivel normativo: Normativa y recomendaciones de seguridad. Está constituido por la normativa y recomendaciones de seguridad que se definan en cada

cve: BOE-A-2021-17235
Verificable en https://www.boe.es

ámbito organizativo de aplicación específico (órganos superiores y directivos, y organismos públicos dependientes a los que sea de aplicación la presente PSI), conforme al artículo 1. La normativa, que comprende los procedimientos, las normas y las instrucciones técnicas de seguridad, es de obligado cumplimiento y se formalizará mediante instrucciones o resoluciones de los titulares de los órganos correspondientes, previa aprobación del presidente del grupo técnico de seguridad de la información, mientras que las recomendaciones consistirán en buenas prácticas y consejos no vinculantes para mejorar las condiciones de seguridad.

Estas normas de seguridad deberán cumplir los siguientes requisitos:

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 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 Esquema Nacional de Seguridad y con el primer nivel normativo enunciado en el presente artículo.

c) Tercer nivel normativo: Procedimientos técnicos. Está constituido por el conjunto de procedimientos técnicos orientados a resolver las tareas, consideradas críticas por el perjuicio que causaría una actuación inadecuada, de seguridad, desarrollo, mantenimiento y explotación de los sistemas de información. Son recomendaciones o informaciones relativas a temas concretos de seguridad basadas en Instrucciones previas, que establecen las configuraciones mínimas de seguridad de los diferentes elementos de un sistema de información, recomendaciones de uso o de otro tipo. La responsabilidad de aprobación de estos procedimientos técnicos dependerá de su ámbito de aplicación, que podrá ser en un ámbito específico o en un sistema de información determinado. Se consideran incluidas en este nivel normativo las guías CCN-STIC elaboradas por el Centro Criptológico Nacional.

Este tercer nivel normativo deberá cumplir los siguientes requisitos:

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 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 Esquema Nacional de Seguridad y con el primer y segundo nivel normativos enunciados en el presente artículo.

2. Además de la normativa enunciada en el presente artículo, 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: informes técnicos, registros, evidencias, buenas prácticas, etc.

3. El personal de cada uno de los órganos u organismos 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.

4. La CMAD establecerá los mecanismos necesarios para compartir la documentación derivada del desarrollo normativo con el propósito de normalizarlo, en la medida de lo posible, en todo el ámbito de aplicación de la PSI.

5. Este marco normativo estará a disposición de todos los miembros del Ministerio de Derechos Sociales y Agenda 2030.

cve: BOE-A-2021-17235
Verificable en https://www.boe.es

Artículo 15. *Gestión de los riesgos.*

1. La gestión de riesgos debe realizarse de manera continua sobre el sistema de información, conforme a los principios de gestión de la seguridad y protección de datos, basada en los riesgos, artículo 6 del Real Decreto 3/2010, de 8 de enero, y artículo 24 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y artículo 28 de la Ley Orgánica 3/2018, de 5 de diciembre y reevaluación periódica, artículo 9 del Real Decreto 3/2010, de 8 de enero, siendo el Responsable del Servicio el encargado de solicitar el preceptivo análisis de riesgos y de que se proponga el tratamiento adecuado, calculando los riesgos residuales. El Responsable de Seguridad, tras la calificación de la información y la determinación del nivel de seguridad del sistema, obtendrá la matriz de aplicabilidad y el conjunto de medidas para garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información y del servicio. Se realizará la evaluación de riesgo, identificando los riesgos residuales y, en base a ellos, se determinará el Plan de Tratamiento de Riesgo, que le será comunicado al Responsable de la Información y del Servicio.

2. El Responsable de Seguridad es el encargado de realizar dicho análisis en tiempo y forma a petición del Responsable del Servicio, así como de identificar carencias y debilidades y ponerlas en conocimiento de los Responsables de la Información y del Servicio.

3. Los Responsables de la Información y del Servicio son los encargados de los riesgos sobre la información y sobre los servicios, respectivamente, siendo responsables de su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.

4. El proceso de gestión de riesgos, que comprende las fases de categorización de los sistemas, análisis de riesgos y selección de medidas de seguridad a aplicar, que deberán ser proporcionales a los riesgos y estar justificadas, deberá revisarse y aprobarse cada año por el titular del órgano o unidad administrativa o, en su caso, organismo adscrito, a través de un Plan de Adecuación al Esquema Nacional de Seguridad.

5. Las indicadas fases del proceso de gestión de riesgos se realizarán según lo dispuesto en los anexos I y II del Real Decreto 3/2010, de 8 de enero, y siguiendo las normas, instrucciones, guías CCN-STIC y recomendaciones para la aplicación del mismo elaboradas por el Centro Criptológico Nacional, así como todo lo referente al análisis de riesgo y de impacto en la protección de datos especificado en el citato Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

Artículo 16. *Protección de datos personales.*

1. En el ámbito del Ministerio de Derechos Sociales y Agenda 2030, la garantía de la protección de datos de carácter personal de las actividades de tratamiento es un objetivo compartido por todas las unidades del Departamento que se rige por los siguientes principios:

a) Licitud, lealtad y transparencia.
b) Limitación de la finalidad.
c) Minimización de datos.
d) Exactitud.
e) Limitación del plazo de conservación.
f) Integridad y confidencialidad.
g) Responsabilidad proactiva.

2. Se aplicarán a los datos personales que sean objeto de tratamiento por parte del Ministerio de Derechos Sociales y Agenda 2030 las medidas de seguridad apropiadas derivadas del análisis de riesgos, así como de las evaluaciones de impacto relativas a la protección de, conforme se detalla en el Reglamento (UE) 2016/679 del Parlamento

cve: BOE-A-2021-17235
Verificable en https://www.boe.es

Europeo y del Consejo, de 27 de abril de 2016, y en la Ley Orgánica 3/2018, de 5 de diciembre.

Además, se aplicarán las medidas correspondientes al anexo II del Real Decreto 3/2010, de 8 de enero.

En el caso de que el análisis de riesgos determine medidas agravadas respecto a la normativa recogida en el anexo II del Real Decreto 3/2010, de 8 de enero, dichas medidas derivadas del análisis de riesgos serán las que se implementarán en la protección de datos personales.

3. En relación con los sistemas de información que, para soportar la prestación de servicios de administración electrónica, manejen datos de carácter personal, prevalecerán las mayores exigencias contenidas en la normativa de protección de datos en vigor que afecte al sistema de información concreto.

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 mismos de la PSI y de su desarrollo normativo.

2. A estos efectos, deberán incluirse actividades formativas en esta materia dentro de los planes de formación del Ministerio de Derechos Sociales y Agenda 2030.

3. La CMAD se encargará de promover las actividades de formación y concienciación en materia de seguridad, según lo indicado en el artículo 6.

Artículo 18. *Actualización permanente y revisiones.*

1. La PSI deberá mantenerse actualizada permanentemente para adecuarla al progreso de los servicios de Administración Electrónica, la evolución tecnológica, el desarrollo de la sociedad de la información, y los estándares internacionales de seguridad.

2. Las propuestas de las sucesivas revisiones de la PSI las hará la Comisión Ministerial de Administración Digital.

Artículo 19. *Terceras partes.*

1. En los casos en que el Ministerio de Derechos Sociales y Agenda 2030 preste servicios o gestione información de otros organismos, se les hará partícipe de la PSI, estableciendo canales para el reporte y coordinación de los respectivos Comités de seguridad y, en su caso, procedimientos de actuación para la reacción ante los ciberincidentes de seguridad.

2. En los casos en que el Ministerio de Derechos Sociales y Agenda 2030 utilice servicios de terceros o les ceda información, se les hará partícipes de esta PSI y de la normativa de seguridad que afecte a dichos servicios o información. Los terceros quedarán sujetos a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para cumplirla. Además, se establecerán procedimientos específicos de reporte y resolución de incidencias y se garantizará que el personal de la tercera parte esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta política.

3. Cuando algún aspecto de la política no pueda ser abordado por una tercera parte según se establece en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad de la Información que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los Responsables de la Información y los Servicios afectados antes de seguir adelante.

cve: BOE-A-2021-17235
Verificable en https://www.boe.es

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

Esta orden deberá mantenerse actualizada para adecuarla al progreso de los servicios de Administración Electrónica, a la evolución tecnológica y al desarrollo de la sociedad de la información, así como a los estándares internacionales de seguridad. Las futuras modificaciones se realizarán a propuesta de la CMAD y requerirán de una orden ministerial, salvo que se trate de la revisión de aspectos técnicos que no requieran de una disposición de carácter general.

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

La aplicación de esta orden no conllevará incremento de gasto público. Las medidas incluidas en la misma no supondrán, en ningún caso, incremento de dotaciones ni de retribuciones ni de otros gastos de personal.

Disposición adicional tercera. *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.*

Se derogan cuantas disposiciones de igual o inferior rango se opongan a lo establecido en la presente orden, y en particular, se considera parcialmente derogada la Orden SSI/321/2014, de 26 de febrero, por la que se aprueba la política de seguridad de la información en el ámbito de la administración electrónica del Ministerio de Sanidad, Servicios Sociales e Igualdad, en todos aquellos aspectos que afecten al Ministerio de Derechos Sociales y Agenda 2030 o a sus organismos adscritos.

Disposición final primera. *Publicidad de la PSI.*

La presente orden se publicará, además de en el «Boletín Oficial del Estado», en la sede electrónica del Ministerio de Derechos Sociales y Agenda 2030 y de sus organismos adscritos.

Disposición final segunda. *Entrada en vigor.*

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

Madrid, 8 de octubre de 2021.–La Ministra de Derechos Sociales y Agenda 2030, Ione Belarra Urteaga.

cve: BOE-A-2021-17235
Verificable en https://www.boe.es