I. DISPOSICIONES GENERALES

MINISTERIO DE DERECHOS SOCIALES, CONSUMO Y AGENDA 2030

2329 *Orden DCA/48/2026, de 23 de enero, por la que se aprueba la Política de Seguridad de la Información en el ámbito de la administración electrónica del Ministerio de Derechos Sociales, Consumo 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 diversos 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, ataques 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 311/2022, de 3 de mayo, 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 12.3 del Real Decreto 311/2022, de 3 de mayo, exige que, en la Administración General del Estado, cada ministerio cuente con su política de seguridad, que aprobará la persona titular del Ministerio. Dicha política se establecerá en base a los principios básicos recogidos en el capítulo II del Esquema Nacional de Seguridad (seguridad como proceso integral; gestión de la seguridad basada en los riesgos; prevención, detección, respuesta y conservación; existencia de líneas de defensa; vigilancia continua; reevaluación periódica; diferenciación de responsabilidades). Además, en su artículo 13 exige que la política de seguridad identifique unos claros responsables de velar por su cumplimiento.

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

Además, el artículo 15 de esta Política de Seguridad de la Información define los tres niveles normativos que se utilizarán para articularla, de forma que se pueda disponer de un corpus normativo común para todos los órganos y organismos que formen parte del ámbito de la Política de Seguridad de la Información.

cve: BOE-A-2026-2329
Verificable en https://www.boe.es

Como requisito fundamental en la aplicación de la Política de seguridad ha de resaltarse el cumplimiento con la legislación en materia de la protección de los datos de carácter personal, lo que permitirá garantizar de forma consistente, la seguridad de los tratamientos de datos personales en base al artículo 32 del 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). En este sentido, la disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, reconoce al Esquema Nacional de Seguridad como un instrumento para la implementación de medidas que permitan garantizar la seguridad de los datos de carácter personal.

Además, cabe reseñar la importancia de que el personal del Ministerio forme parte activa de ejecución de los mecanismos y buenas prácticas para garantizar la seguridad de la información en el ámbito corporativo. En particular, el artículo 18, reconoce la necesidad de que el personal cuente con la información y formación adecuadas, y conozca sus responsabilidades y deberes al respecto.

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, Consumo y Agenda 2030, y da cumplimiento al mandato contenido en el artículo 12.3 del Real Decreto 311/2022, de 3 de mayo.

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, Consumo y Agenda 2030. Cumple también con el principio de transparencia, ya que identifica claramente su propósito. Al tratarse de una norma puramente organizativa, su tramitación no ha requerido de consulta pública previa y de los trámites de audiencia e información pública. 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, Consumo y Agenda 2030 y de la Agencia Española de Protección de Datos.

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

Artículo 1. *Objeto.*

La Política de Seguridad de la Información (en adelante, PSI) es el conjunto de directrices que rigen la forma en que la organización gestiona y protege la información que trata y los servicios que presta.

De acuerdo con lo previsto en el artículo 12.3 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, el objeto de la presente orden es la aprobación de la PSI en el ámbito de la Administración Electrónica del Ministerio de Derechos Sociales, Consumo y Agenda 2030, así como el establecimiento del marco organizativo y tecnológico de la misma.

Artículo 2. *Ámbito de aplicación.*

1. Esta política se aplica y será de obligado cumplimiento para todos los órganos del Ministerio de Derechos Sociales, Consumo y Agenda 2030, así como a todos los organismos públicos y entidades de derecho público vinculados o dependientes que no tengan establecida su propia política de seguridad.

2. La PSI se aplica a todos los sistemas de información que gestionen las diferentes unidades de los órganos directivos o entidades y organismo adscritos al Ministerio de

cve: BOE-A-2026-2329
Verificable en https://www.boe.es

Derechos Sociales, Consumo y Agenda 2030. Además, 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 con el mismo.

En el ámbito de esta PSI, se debe entender por personal a cualquier empleado público perteneciente al Ministerio de Derechos Sociales, Consumo y Agenda 2030 o a los organismos y entidades gestoras dependientes o adscritos al mismo. Además, el personal de las entidades colaboradoras, de empresas contratadas o de encargos a medios propios con vinculación con los centros directivos del Ministerio de Derechos Sociales, Consumo y Agenda 2030 y de los organismos y entidades dependientes o adscritos, también tendrán la consideración de personal relacionado con la PSI.

Artículo 3. *Misión de la organización.*

Corresponde al Ministerio de Derechos Sociales, Consumo y Agenda 2030, según lo establecido en Real Decreto 209/2024, de 27 de febrero, por el que se establece la estructura orgánica básica del Ministerio de Derechos Sociales, Consumo y Agenda 2030:

1. La propuesta y ejecución de la política del Gobierno en materia de derechos sociales y bienestar social, de familia y de su diversidad, de cohesión social, de atención a las personas dependientes o con discapacidad, así como de protección de los derechos y del bienestar de los animales.
2. Igualmente, corresponde al Ministerio de Derechos Sociales, Consumo y Agenda 2030 la propuesta y ejecución de la política del Gobierno en materia de consumo, protección de las personas consumidoras y regulación del juego.
3. Asimismo, corresponde al Ministerio de Derechos Sociales, Consumo y Agenda 2030 la propuesta y ejecución de la política del Gobierno en materia de impulso, seguimiento y cooperación para la implementación de la Agenda 2030 y el cumplimiento de los Objetivos de Desarrollo Sostenible.

Artículo 4. *Marco normativo.*

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

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 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad y las Instrucciones Técnicas de Seguridad para su aplicación dictadas por la persona titular de la Secretaría de Estado de Función Pública, de acuerdo con lo previsto en la disposición adicional segunda de dicho real decreto.
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 (Reglamento General de Protección de Datos, en adelante RGPD).
7. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
8. Real Decreto 255/2025, de 1 de abril, por el que se regula el documento nacional de identidad.

cve: BOE-A-2026-2329
Verificable en https://www.boe.es

9. La legislación sectorial reguladora de la actuación de los órganos superiores y directivos del Ministerio de Derechos Sociales, Consumo y Agenda 2030, según lo establecido en Real Decreto 209/2024, de 27 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio de Derechos Sociales, Consumo y Agenda 2030.

10. Orden DCA/1495/2024, de 23 de diciembre, por la que se crea y regula la Comisión Ministerial de Administración Digital del Ministerio de Derechos Sociales, Consumo y Agenda 2030.

11. Resolución de 24 de febrero de 2010, del Instituto de Mayores y Servicios Sociales, por la que se crea y regula la sede y el registro electrónicos 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.

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

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

18. El Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.

19. El Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información que traspone la Directiva Europea NIS (Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016).

20. El 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.

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

Artículo 5. *Principios de la seguridad de la información.*

Los principios básicos y requisitos de la seguridad de la información desarrollados bajo el marco de esta Política de Seguridad son los recogidos en el Esquema Nacional de Seguridad regulado por el Real Decreto 311/2022, de 3 de mayo, en particular, los previstos en sus capítulos II y III, y su normativa de desarrollo.

Artículo 6. *Organización de la seguridad.*

La estructura organizativa para la gestión de la seguridad de la información en el ámbito descrito por la PSI del Ministerio de Derechos Sociales, Consumo y Agenda 2030 está compuesta por los siguientes agentes:

1. Comisión Ministerial de Administración Digital (CMAD).
2. Responsable de la Seguridad (RSeg).
3. Comité de Seguridad de la Información (CSI).
4. Responsable de la Información (RInf).
5. Responsable del Servicio (RSer).
6. Responsable del Sistema (RSis).

cve: BOE-A-2026-2329
Verificable en https://www.boe.es

Artículo 7. *La Comisión Ministerial de Administración Digital.*

1. De acuerdo con lo previsto en el artículo 5 del Real Decreto 1125/2024, de 5 de noviembre, por el que se regulan la organización y los instrumentos operativos para la Administración Digital de la Administración del Estado, 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.

2. De acuerdo con lo previsto en el artículo 5.1 de la Orden DCA/1495/2024, de 23 de diciembre, por la que se crea y regula la Comisión Ministerial de Administración Digital del Ministerio de Derechos Sociales, Consumo y Agenda 2030, ésta será la encargada de realizar las siguientes funciones relacionadas con la seguridad:

a) Impulsar la seguridad de la información en la organización, aportando los recursos necesarios y apoyando a los distintos roles de seguridad de la información.

b) Aplicar las directrices de seguridad establecidas por el Esquema Nacional de Seguridad (en adelante ENS) y demás legislación vigente en el ámbito de la seguridad de la información y las comunicaciones, así como supervisar su cumplimiento.

c) Elaborar la estrategia de la organización en lo que respecta a seguridad de la información y promover la mejora continua en la gestión de la misma.

d) Impulsar y velar por el cumplimiento de la PSI y de su desarrollo normativo. Así como aprobar las propuestas de modificación de esta y velar por su actualización permanente.

e) 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. Así como aprobar el nombramiento del Responsable de la Seguridad y del Responsable del Sistema.

f) Aprobar las normas de desarrollo de segundo nivel de la PSI, según lo previsto en el artículo 15.

g) Aprobar el Plan de Auditoría y el Plan de Formación propuestos por el Responsable de la Seguridad, así como ordenar la realización de las auditorías o autoevaluaciones de seguridad y recibir información de los resultados de las mismas.

h) 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.

i) 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.

j) 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.

k) Apoyar la coordinación, cooperación y colaboración con la Agencia Estatal de Administración Digital y otras Administraciones públicas en materia de seguridad de la información.

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.

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 estas.

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

cve: BOE-A-2026-2329
Verificable en https://www.boe.es

Artículo 8. *Responsable de la Seguridad.*

1. Conforme a lo dispuesto en el artículo 13.2.c) del Real Decreto 311/2022, de 3 de mayo, el Responsable de la Seguridad 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 la seguridad de la información manejada, de los servicios electrónicos prestados por los sistemas de información y la protección de datos de carácter personal, además de reportar sobre estas cuestiones a la CMAD.

Cada órgano superior o directivo del Ministerio de Derechos Sociales, Consumo y Agenda 2030, así como los organismos y entidades adscritas al Departamento ministerial podrán designar un responsable de la seguridad. La designación deberá ser notificada a la CMAD. En ausencia de una designación las funciones de responsable de la seguridad serán asumidas por el Comité de Seguridad de la Información.

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

2. Serán deberes y responsabilidades del Responsable de la Seguridad las siguientes:

a) Promover y mantener el nivel adecuado de seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información en su ámbito de responsabilidad.

b) Promover la formación y concienciación en materia de seguridad de la información.

c) Elaborar la normativa de seguridad de segundo nivel definida en el artículo 15 y proponer su aprobación al Pleno de la CMAD.

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

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

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

g) 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.

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

i) Impulsar la mejora continua en la gestión de la seguridad de la información.

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

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 311/2022, de 3 de mayo, asigne al Responsable de la Seguridad.

3. El Responsable de la Seguridad será distinto del Responsable del Sistema, no debiendo existir dependencia jerárquica entre ambos. En aquellas situaciones excepcionales en las que la ausencia justificada de recursos requiera que ambas funciones recaigan en la misma persona o en distintas personas con relación jerárquica, se aplicarán medidas compensatorias para garantizar la finalidad del principio de diferenciación de responsabilidades previsto en el artículo 11 del Real Decreto 311/2022, de 3 de mayo.

cve: BOE-A-2026-2329
Verificable en https://www.boe.es

Artículo 9. *Comité de Seguridad de la Información.*

1. El Comité de Seguridad de la Información del Ministerio de Derechos Sociales, Consumo y Agenda 2030 (en adelante, CSI), tiene la responsabilidad de dar seguimiento y alinear las actividades en materia de seguridad del Ministerio, además de participar en la gestión de proyectos de mejora continua, continuidad del servicio y el cumplimiento de las medidas definidas para la obtención y mantenimiento de las diferentes certificaciones.

2. El CSI, órgano colegiado que se adscribe a la Subsecretaría, ejercerá las funciones del Responsable de la Seguridad, para todos los centros directivos del departamento ministerial que no notifiquen una designación de responsable de la seguridad a la CMAD y estará compuesto por:

a) Presidencia: La persona titular 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 la persona titular de la Vicepresidencia.

b) Vicepresidencia. La persona titular de la coordinación del Área de Seguridad de la Información de la División de Tecnologías de la Información y Comunicaciones, que tendrá voz y voto. En caso de ausencia, vacante o enfermedad será sustituido por la persona titular de la División de Control de Juego Seguro.

c) Secretaría: La persona titular de la Jefatura de Área de Infraestructuras de la División de Tecnologías de la Información y Comunicaciones, 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. 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) Vocales: la persona titular de la División de Control de Juego Seguro y una persona representante de cada uno de los organismos y entidades públicos adscritos en el ámbito del Ministerio, que tendrán voz y voto. Los vocales representantes de los organismos públicos, así como sus sustitutos, serán designados por la persona titular de la dirección del organismo o entidad al que representen.

3. Cuando la complejidad, distribución, separación física de sus elementos o número de usuarios de los sistemas de información lo justifiquen, el CSI 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.

4. El CSI 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. Sus miembros serán renovados cada cuatro años o con ocasión de vacante.

5. A requerimiento del CSI se convocará cualquier otro responsable o responsables, propio o de terceras organizaciones subcontratadas para la prestación de los servicios, cuya intervención sea precisa por estar afectados por el ENS y por la regulación en materia de Protección de Datos.

6. A las reuniones del CSI, podrán acudir representantes designados por los Delegados de Protección de Datos del Ministerio 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. Puntualmente se podrá invitar a personal técnico propio o externo a las reuniones.

7. En el seno del CSI, 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 CSI.

cve: BOE-A-2026-2329
Verificable en https://www.boe.es

8. El CSI colaborará con la CMAD en las cuestiones que ésta le encomiende y en particular ejercerá las siguientes funciones, que podrán ser ampliadas dentro su ámbito competencial:

a) Implantar las directrices de la CMAD dentro del ámbito de seguridad de la información.
b) Preparar las normas y procedimientos en materia de seguridad de la información. Elaborar, promover y mantener la política de seguridad de la información y proponer su aprobación al Pleno de la Comisión.
c) Validar el Plan de Seguridad y presentarlo a la CMAD para que sea aprobado.
d) Supervisar el desarrollo y mantenimiento del Plan de Continuidad de negocio.
e) Velar por el cumplimento de la legislación y regulación vigente.
f) Promover la concienciación y formación de los empleados en materia de seguridad de la información.
g) Gestionar, coordinar y supervisar, en conjunto con otros departamentos ministeriales, la ciberseguridad de todas las actividades relacionadas con la seguridad de las TIC del Ministerio.
h) Seguimiento y control de la gestión de incidentes de seguridad.
i) Validar la correcta ejecución de los planes de acción y ciclo de mejora continua de cara a la seguridad de la información y protección de datos personales.
j) Hacer partícipe al Delegado de Protección de Datos (DPD) en caso de afectación sobre datos personales.
k) Elaborar el plan de riesgos y las posibles soluciones para mitigar las amenazas.
l) Proponer nuevos objetivos en materia de seguridad de la información.
m) Velar por el cumplimiento de la documentación de seguridad, manteniéndola organizada y actualizada, así como de gestionar los mecanismos de acceso a la misma.
n) Validar la implantación de los requisitos de seguridad necesarios.
ñ) Establecer los controles y las medidas técnicas y organizativas para asegurar los sistemas de información y revisar periódicamente el estado de la seguridad de la información.
o) Controlar que las auditorías de seguridad se realicen con la frecuencia necesaria.
p) Reportar a la CMAD y Comité de Seguridad de los demás departamentos ministeriales las cuestiones relevantes en materia de seguridad de la información del Ministerio.

Artículo 10. *Responsable de la Información.*

1. En base a lo dispuesto en el artículo 13.2 a) del Real Decreto 311/2022, de 3 de mayo, el Responsable de la Información determinará los requisitos de la información tratada por la organización en materia de seguridad, es decir, determinará y aprobará los niveles de seguridad aplicables a la información. Si esta información incluye 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 RGPD.
2. Serán deberes y responsabilidades del Responsable de la Información, las siguientes:

a) Determinar, respecto de la información, los niveles en cada dimensión de seguridad según el marco establecido en el anexo I del ENS y valorar el impacto de los incidentes que afecten a la seguridad de la información.
b) Se encargará, junto al Responsable 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) Será responsable 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-2026-2329
Verificable en https://www.boe.es

3. Los órganos superiores o directivos del Ministerio y los órganos responsables de los organismos y entidades vinculados o dependientes que no cuenten con PSI propia, designarán al Responsable o Responsables de la Información, 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 la Seguridad.

4. A los efectos previstos en el RGPD, y en la medida en que sea el que determine, sólo o junto con otros, los fines y medios del correspondiente tratamiento de datos personales, el Responsable de la Información podrá tener la consideración de responsable o encargado del tratamiento respecto de los datos personales contenidos en la información incluida en su ámbito de actuación. Cuando se dé esta circunstancia, el Responsable de la Información deberá mantener los registros de las actividades de tratamiento a los que se refiere el artículo 30 del RGPD.

5. Este rol podrá coincidir con el Responsable del Servicio. De igual forma, este rol no podrá coincidir con el de Responsable del Sistema.

Artículo 11. *Responsable del Servicio.*

1. De acuerdo con lo previsto en el artículo 13.2.b) del Real Decreto 311/2022, de 3 de mayo, se asigna al Responsable del Servicio la potestad de establecer los requisitos del servicio en materia de seguridad, es decir, la potestad de determinar y aprobar los requisitos aplicables al servicio en cada dimensión de seguridad.

2. Serán deberes y responsabilidades del Responsable del Servicio, las siguientes:

a) Tiene la responsabilidad última de la prestación de un cierto nivel de servicio y su protección, para ello debe contar con las competencias suficiente para decidir sobre la finalidad y prestación de dicho servicio.

b) Dentro del marco establecido Real Decreto 311/2022, de 3 de mayo, tiene la potestad de establecer y aprobar los requisitos del servicio en materia de seguridad.

3. El Responsable de la Información y el Responsable del Servicio coincidirán cuando la prestación del servicio dependa de la unidad que es responsable de la información o cuando el servicio no maneje información de diferentes procedencias. Sin embargo, su diferenciación tendrá sentido si se cumplen los siguientes puntos:

a) Cuando el servicio maneja información de diferentes procedencias, no necesariamente de la misma unidad departamental que la que presta el servicio.

b) Cuando la prestación del servicio no depende de la unidad que es responsable de la información.

4. Los órganos superiores o directivos del Ministerio, y los órganos responsables de los organismos y entidades vinculados o dependientes que no cuenten con PSI propia, designarán al Responsable o Responsables de los servicios, 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 la Seguridad.

5. Este rol no podrá coincidir con el de Responsable de la Seguridad, ni con el de Responsable del Sistema, ni siquiera cuando se trate de organizaciones de reducida dimensión que funcionen de forma autónoma.

Artículo 12. *Responsable del Sistema.*

1. De acuerdo con lo previsto en el artículo 13.2.d) del Real Decreto 311/2022, de 3 de mayo, el Responsable del Sistema, por sí o mediante recursos propios o contratados, desarrollará la forma concreta de implementar la seguridad en el sistema y la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad.

cve: BOE-A-2026-2329
Verificable en https://www.boe.es

2. Serán deberes y responsabilidades del Responsable del Sistema, las siguientes:

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) Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento. Pudiendo delegar en administradores u operadores bajo su responsabilidad.
d) Proponer la suspensión del tratamiento de una cierta información o la prestación de un determinado servicio si aprecia deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos.

3. La CMAD, será la encargada de designar este perfil de acuerdo con su propia organización interna, sin que, esto implique, en ningún caso, un aumento de las actuales dotaciones ni de las retribuciones de dichos efectivos por ningún concepto. Se comunicará el nombramiento o nombramientos al Responsable de la Seguridad.
4. El rol de Responsable del Sistema no podrá coincidir con el de Responsable de la Información, Responsable del Servicio ni con el de Responsable de la Seguridad de la Información.

Artículo 13. *Resolución de conflictos.*

1. La resolución de conflictos entre los diferentes responsables, serán resueltos por el superior jerárquico de los mismos. En su defecto, será la CMAD quien resuelva.
2. En la resolución de estos conflictos, prevalecerán las mayores exigencias derivadas de la protección de datos de carácter personal.

Artículo 14. *Obligaciones del personal.*

1. Todo el personal que presta servicios en el Ministerio de Derechos Sociales, Consumo y Agenda 2030 y sus organismos y entidades 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, Consumo 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 15. *Gobernanza de la estructura normativa.*

1. El cuerpo normativo sobre seguridad de la información es de obligado cumplimiento y se estructura en los siguientes niveles relacionados jerárquicamente, según su ámbito de aplicación y grado de detalle técnico, de manera que cada norma de un determinado nivel de desarrollo se fundamente en las normas de nivel superior:

a) Primer nivel normativo:

Está constituido por la presente Política de Seguridad de la Información y las directrices generales de seguridad de la información aplicables a los órganos del Ministerio y los organismos y entidades comprendidos en el ámbito de esta PSI.

cve: BOE-A-2026-2329
Verificable en https://www.boe.es

b) Segundo nivel normativo:

Está constituido por la normativa y las recomendaciones de seguridad de la información, en desarrollo de la PSI, que se definan para cada ámbito organizativo de aplicación específico. Dicho ámbito podrá corresponder a uno o más órganos superiores o directivos del Ministerio, así como a los órganos responsables de los organismos o entidades de derecho público vinculados o dependientes.

En cuanto a la normativa de seguridad de la información de este segundo nivel, comprenderá la regulación de procedimientos sobre «Seguridad en las Tecnologías de la Información y las Comunicaciones» (en adelante, STIC), y normas e instrucciones técnicas STIC, dictadas, por las personas titulares de los órganos superiores o directivos del ministerio y de las personas responsables de los organismos y entidades adscritas o dependientes en cuyo ámbito se hayan de aplicar.

En cuanto a las recomendaciones, versarán sobre buenas prácticas y consejos no vinculantes para la mejora de las condiciones de seguridad de la información en soporte electrónico. Las recomendaciones las propone el Responsable de la Seguridad, dentro de su ámbito de competencia, y las aprueba la CMAD.

c) Tercer nivel normativo: Procesos y Procedimientos Técnicos.

Corresponden al desarrollo del segundo nivel normativo y está constituido por Procesos y Procedimientos que detallan los aspectos técnicos para realizar una determinada tarea respetando los principios de seguridad de la información de la organización y los procesos internos en ella establecidos. Incluyen aspectos de configuración, implementación y tecnológicos relativos a la seguridad, desarrollo, mantenimiento y explotación de los sistemas de información.

Su ámbito de aplicación podrá ser general o corresponder a un ámbito orgánico específico o un sistema de información determinado. La aprobación de los Procedimientos técnicos corresponde al Responsable de la Seguridad.

Se consideran incluidas en este nivel normativo:

i. Las guías de seguridad de las tecnologías de la información y la comunicación elaboradas por el Centro Criptológico Nacional (en adelante guías CCN-STIC).

ii. Las normas o recomendaciones aprobadas por órganos y organismos con competencias regulatorias en materia de seguridad o de protección de datos, como son el Centro Criptológico Nacional, la Secretaría de Estado de Digitalización e Inteligencia Artificial, la Agencia Estatal de Administración Digital, o la AEPD.

iii. Conjunto de procedimientos técnicos elaborados y aprobados por los Responsables de Seguridad en sus ámbitos de actuación.

iv. Recomendaciones, guías de configuración y buenas prácticas publicadas por organismos u organizaciones internacionales y por los fabricantes de productos de seguridad.

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

3. 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.

4. El cuerpo normativo de seguridad se encontrará a disposición del personal de la organización, teniendo en cuenta los principios de mínimo privilegio y de necesidad de conocer y responsabilidad de compartir. Además, estará sujeto a revisiones periódicas para garantizar su actualización.

cve: BOE-A-2026-2329
Verificable en https://www.boe.es

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

1. El tratamiento de datos de carácter personal en el ámbito del Ministerio de Derechos Sociales, Consumo y Agenda 2030 se efectuará conforme a los principios de licitud, transparencia y lealtad, finalidad, minimización, exactitud, limitación del plazo de conservación, integridad y confidencialidad, así como responsabilidad proactiva y seguridad.

2. Se aplicarán a los datos de carácter personal que sean objeto de tratamiento por parte de los órganos superiores y directivos del Ministerio de Derechos Sociales, Consumo y Agenda 2030, además de los órganos responsables de los organismos y entidades adscritas o dependientes, ya sean tratamientos automatizados o no automatizados, las medidas de seguridad técnicas y organizativas apropiadas derivadas del análisis de riesgos, así como de las evaluaciones de impacto relativas a la protección de datos personales, conforme se detalla 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). Además, en cumplimiento de la disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre, se aplicarán las medidas de seguridad correspondientes a la categoría del Sistema según el anexo II del 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. En el caso de que el análisis de riesgos determine medidas agravadas respecto a la normativa recogida en el anexo II del Real Decreto 311/2022, de 3 de mayo, dichas medidas derivadas del análisis de riesgos serán las que se implementarán en la protección de datos de carácter personal.

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. *Gestión de los riesgos.*

1. La gestión de riesgos debe realizarse de manera continua sobre los sistemas de información, conforme a los principios de gestión de la seguridad y protección de datos, basada en los riesgos y al principio de vigilancia continua y reevaluación periódica, reconocidos por la legislación vigente en materia de seguridad de la información y protección de datos personales, 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 la Seguridad, tras la calificación de la información y la determinación del nivel de seguridad del sistema, obtendrá la declaración 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 la 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, así como de la CMAD.

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 validarse cada año por el titular del órgano o unidad administrativa o, en su caso, organismo dependiente o adscrito.

cve: BOE-A-2026-2329
Verificable en https://www.boe.es

5. Los análisis de riesgos, así como su tratamiento, se realizarán también cuando se detecten incidentes de seguridad o se identifiquen cambios organizativos, metodológicos, legales o tecnológicos que pudieran suponer un incremento del riesgo al que se encuentren expuestos los activos.

6. Las indicadas fases del proceso de gestión de riesgos se realizarán según lo dispuesto en los anexos I y II del Real Decreto 311/2022, de 3 de mayo, y siguiendo las normas, instrucciones, guías CCN-STIC y recomendaciones para la aplicación de este, elaboradas por el Centro Criptológico Nacional.

7. Al menos con una periodicidad anual, y siempre que se realicen modificaciones sustanciales en los sistemas de información, la CMAD aprobará la definición de las medidas de seguridad, las cuales se deberán reevaluar y actualizar, de modo que su eficacia esté adaptada a la constante evolución de los riesgos y sistemas de protección.

8. Los análisis de riesgos y de impacto, desde el enfoque relativo a la protección de datos especificado en RGPD, se realizarán según lo establecido en la normativa vigente en materia de protección de datos personales, debiendo seguir también las indicaciones de la Agencia Española de Protección de Datos y demás autoridades competentes al respecto.

Artículo 18. *Formación y concienciación.*

1. Todo el personal relacionado con la información, los servicios y los sistemas de información, deberá ser formado e informado de sus deberes y obligaciones en materia de seguridad de la información.

2. Para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios del Ministerio de Derechos Sociales, Consumo y Agenda 2030, se articularán los mecanismos necesarios para llevar a la práctica la concienciación y la formación específica necesaria e imprescindible en todos los niveles de la organización, así como a la difusión de la PSI y de su desarrollo normativo.

Artículo 19. *Política de seguridad de la información de los organismos y entidades vinculados, dependientes o adscritos al Ministerio de Derechos Sociales, Consumo y Agenda 2030.*

1. De acuerdo con lo previsto en el artículo 12.3 del Real Decreto 311/2022, de 3 de mayo, y el apartado 1 del artículo 2 de esta PSI, los organismos y entidades vinculados, dependientes o adscritos al Ministerio de Derechos Sociales, Consumo y Agenda 2030 podrán contar con su propia política de seguridad, aprobada por el órgano competente, que será coherente con la del Departamento aprobada por esta orden.

2. En caso de discrepancia, prevalecerá la política de seguridad de la información definida en esta orden ministerial.

3. En todo caso, los organismos públicos o entidades vinculados o dependientes del Departamento deberán informar de forma inmediata a la División de Tecnologías de la Información y Comunicaciones sobre cualquier incidencia o riesgo que pueda poner en peligro la seguridad de los sistemas informáticos del Departamento.

Artículo 20. *Terceras partes.*

1. En los casos en que el Ministerio de Derechos Sociales, Consumo y Agenda 2030 preste servicios o gestione información de otros organismos, se les hará partícipes de la PSI y de la normativa de seguridad que afecte a dichos servicios o información, 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, Consumo y Agenda 2030 utilice servicios de terceros o les ceda información, se les hará partícipes de la 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

cve: BOE-A-2026-2329
Verificable en https://www.boe.es

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 y formado 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 la 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.

4. 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.

5. Corresponde al delegado de Protección de Datos (DPD) del Ministerio de Derechos Sociales, Consumo y Agenda 2030 informar y asesorar a los Responsables del Tratamiento de las obligaciones que les incumben en virtud del RGPD, además de supervisar el cumplimiento de la normativa en materia de protección de datos de carácter personal del departamento, ofrecer asesoramiento y actuar como interlocutor de los Responsables del Tratamiento con la Agencia Española de Protección de Datos.

Disposición adicional primera. *Revisión y Actualización de la PSI.*

La Política de Seguridad de la Información que aprueba esta orden deberá mantenerse actualizada para adecuarla a la evolución normativa, al progreso de los servicios de la administración, a la evolución tecnológica y al desarrollo de la sociedad de la información, así como a los estándares internacionales de seguridad y las guías de seguridad de las tecnologías de la información y las comunicaciones.

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

La aplicación de esta orden no conllevará incremento del gasto público. Las medidas incluidas en la presente orden no supondrán incremento de dotaciones ni de retribuciones ni de otros gastos de personal.

Disposición derogatoria única. *Derogación normativa.*

Quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo establecido en la presente orden, y en particular, la 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, así como la Orden CSM/418/2022, de 10 de mayo, por la que se aprueba la Política de Seguridad de la Información en el ámbito de la administración electrónica del Ministerio de Consumo.

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, Consumo 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, 23 de enero de 2026.–El Ministro de Derechos Sociales, Consumo y Agenda 2030, Pablo Bustinduy Amador.

cve: BOE-A-2026-2329
Verificable en https://www.boe.es