I. DISPOSICIONES GENERALES

MINISTERIO DE POLÍTICA TERRITORIAL Y MEMORIA DEMOCRÁTICA

13949 *Orden TMD/651/2026, de 23 de junio, por la que se aprueba la Política de Seguridad de la Información del Ministerio de Política Territorial y Memoria Democrática.*

La Orden TAP/3148/2011, de 7 de octubre, por la que se aprueba la Política de Seguridad de la Información en el ámbito de la Administración electrónica del Ministerio de Política Territorial y Administración Pública, supuso la aprobación de la Política de Seguridad de la Información en el ámbito de la Administración electrónica del extinto Ministerio de Política Territorial y Administración Pública, así como el establecimiento del marco organizativo y tecnológico de la misma.

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.

Por su parte, 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.

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

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, en adelante ENS, 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 del ENS, exige que cada ministerio cuente con su política de seguridad, que aprobará la persona titular del Departamento. Esta política de seguridad se establecerá con base en los principios básicos recogidos en el capítulo II del ENS (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 y diferenciación de responsabilidades) y desarrollará una serie de requisitos mínimos consignados en el ya mencionado artículo 12.

El Reglamento General de Protección de Datos, 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, en adelante RGPD, señala que la protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos de dicho reglamento. A fin de poder demostrar la conformidad con el RGPD, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan, en particular, los principios de protección de datos desde el diseño y por defecto.

cve: BOE-A-2026-13949
Verificable en https://www.boe.es

A tal efecto establece, en su artículo 24, como obligaciones generales del responsable del tratamiento y del encargado del tratamiento, la aplicación de las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el citado RGPD. Entre las medidas mencionadas se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas medidas para la protección de datos.

Además de en el marco de las normas mencionadas con anterioridad esta orden se dicta también de acuerdo con lo dispuesto en 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, que señala que en el ámbito del sector público el ENS incluirá las medidas que deban implantarse en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del RGPD en orden a aplicar las medidas de seguridad al tratamiento de datos personales.

Con relación a la ciberseguridad, el Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones, incorpora medidas para la seguridad pública, asegurando aspectos relacionados con la mayor exposición a ciberamenazas que exigen una mejor protección de redes y sistemas, así como de la privacidad y los derechos digitales de las personas.

Respecto al marco normativo europeo, la Directiva NIS 2, Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148, establece obligaciones de ciberseguridad para los Estados miembros, medidas para la gestión de riesgos de ciberseguridad y obligaciones de notificación para las entidades comprendidas en su ámbito de aplicación, así como obligaciones referentes al intercambio de información sobre ciberseguridad y obligaciones de supervisión y ejecución para los Estados miembros.

Por otra parte, el marco normativo vigente en el ámbito de la prestación de servicios electrónicos a los ciudadanos, en materia de Política de Seguridad de la Información y de protección de datos personales, así como la actual organización administrativa, determinan la necesidad de dictar esta orden por la que se aprueba la Política de Seguridad de la Información y de los servicios en el ámbito de la administración digital del Ministerio de Política Territorial y Memoria Democrática y se crea, en este Departamento, el Comité de Seguridad de las Tecnologías de la información y las Comunicaciones.

Esta orden cumple con los principios de buena regulación, de necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia y eficiencia recogidos en el artículo 129 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

En primer lugar, en virtud de los principios de necesidad y eficacia, esta iniciativa normativa está justificada por las razones expuestas y es el instrumento más adecuado para dar cumplimiento al mandato contenido en el artículo 12.3 del ENS. Además, se ajusta al principio de proporcionalidad, en tanto que la norma contiene la regulación imprescindible para atender sus objetivos. Se garantiza el principio de seguridad jurídica, en tanto que la norma es coherente con el resto del ordenamiento jurídico y, en particular, con el marco regulatorio en el ámbito de la Política de Seguridad de la Información. Cumple con el principio de transparencia, ya que identifica claramente su propósito y, al tratarse de una norma organizativa su tramitación no ha requerido de la consulta pública previa ni de los trámites de audiencia e información pública. Finalmente, es también adecuada al principio de eficiencia, ya que no impone cargas administrativas.

Esta orden se dicta en cumplimiento del artículo 12 ENS. En su tramitación se ha recabado el informe de la Agencia Española de Protección de Datos y de la Comisión Ministerial de Administración Digital del Departamento.

cve: BOE-A-2026-13949
Verificable en https://www.boe.es

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

Artículo 1. *Objeto y ámbito de aplicación.*

1. De acuerdo con lo previsto en el artículo 12.3 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, en adelante ENS, el objeto de esta orden es aprobar la Política de Seguridad de la Información, en adelante PSI, en el ámbito de la Administración electrónica y de la protección de datos personales del Ministerio de Política Territorial y Memoria Democrática, en adelante MPTMD, así como el marco organizativo y tecnológico de la misma.

2. De acuerdo con lo previsto en los artículos 12.2, 12.3 y 13.1 del ENS y el Real Decreto 273/2024, de 19 de marzo, por el que se desarrolla la estructura orgánica básica del Ministerio de Política Territorial y Memoria Democrática, el ámbito subjetivo de esta PSI comprende todos los órganos centrales y servicios territoriales integrados en el Departamento.

3. Esta PSI será de obligado cumplimiento para todo el personal del MPTMD, siendo aplicable a todos los sistemas de información y, en general, a toda la información que sea gestionada por el Departamento, con independencia de cuál sea su soporte, destino, adscripción o relación con el mismo, así como a toda aquella persona que acceda a ella.

4. En el caso de materias clasificadas, será de aplicación su normativa específica y los procedimientos habilitados para su protección, sin que la presente PSI altere dicho régimen.

Artículo 2. *Misión del Departamento.*

El MPTMD es el Departamento de la Administración General del Estado al que le corresponde la propuesta y ejecución de la política del Gobierno de la Nación en materia de relaciones y cooperación con las comunidades autónomas y las entidades que integran la administración local y las competencias relativas a la organización territorial del Estado; así como las relaciones con las Delegaciones y Subdelegaciones del Gobierno y las Direcciones insulares, y el apoyo a su gestión. Asimismo, a este Departamento le corresponde la propuesta y ejecución de la política del Gobierno en materia de memoria histórica y democrática.

Artículo 3. *Marco normativo.*

1. El marco jurídico en que se desarrollan las actividades del MPTMD en relación con la gestión y protección de la información que trata y los servicios que presta, sin perjuicio de la legislación específica, está integrado fundamentalmente por las siguientes normas:

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

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

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

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

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

f) 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.

cve: BOE-A-2026-13949
Verificable en https://www.boe.es

g) 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.

h) 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 aprobadas por la persona titular del Ministerio para la Transformación Digital y de la Función Pública de acuerdo con lo previsto en la disposición adicional segunda de dicho real decreto.

i) 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.

j) 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.

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

l) 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.

m) La Directiva NIS2, 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, por la que se modifican el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148.

n) Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial), en adelante RIA.

2. También forman parte del marco normativo las restantes normas aplicables a la Administración electrónica del Departamento derivadas de las anteriores y publicadas en su sede electrónica asociada.

Artículo 4. *Funciones del Departamento.*

Según el Real Decreto 273/2024, de 19 de marzo, y la Orden TMD/1036/2024, de 23 de septiembre, por la que se crea y regula la Comisión Ministerial de Administración Digital del MPTMD, los objetivos del Departamento relativos a la prestación de sistemas de información y servicios se encuadran en los siguientes ejes de actuación que corresponden, por un lado, a la Subsecretaría de Política Territorial y Memoria Democrática a través de la División de Tecnologías de la Información; por otro a la Agencia Estatal de Administración Digital, en lo que concierne a la provisión de aplicaciones y servicios en materia TIC prestados a las Delegaciones y Subdelegaciones del Gobierno y a las Direcciones insulares, de acuerdo con lo previsto en el artículo 16.c).5.º de su Estatuto, aprobado por el Real Decreto 1118/2024, de 5 de noviembre y, por último, a la Comisión Ministerial de Administración Digital como órgano colegiado para la coordinación interna de la política del Departamento en materia de tecnologías de la información y Administración electrónica:

a) Dirección y coordinación de los desarrollos de los sistemas de información; la elaboración, preparación y propuesta de necesidades de los recursos tecnológicos; así como la prestación de servicios en materia de tecnologías de la información y la dirección y coordinación del portal de internet, de la sede electrónica asociada y de la Intranet.

b) Elaboración, desarrollo y ejecución de los planes de digitalización del Departamento, así como la implantación y seguimiento de los planes de trasformación digital de la Administración General del Estado, en coordinación con la Agencia Estatal de Administración Digital.

cve: BOE-A-2026-13949
Verificable en https://www.boe.es

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

1. La PSI aplicará los principios básicos que se establecen en el ENS en el ámbito de la Administración electrónica, de acuerdo con el interés general, naturaleza y complejidad de la materia regulada, permitiendo una protección adecuada de la información y de los servicios.

2. Atendiendo al ENS, el MPTMD implementará diversas medidas de seguridad proporcionales a la naturaleza de la información y de los servicios a proteger, teniendo en cuenta la categoría de los sistemas afectados bajo los siguientes principios:

a) Protección de datos personales. Se adoptarán las medidas técnicas y organizativas destinadas a garantizar el nivel de seguridad exigido por la normativa vigente en relación con el tratamiento de datos de carácter personal tal y como se establece en el artículo 32 del RGPD y en el artículo 28 LOPDGDD. Dichas medidas deberán ser proporcionales en función del análisis de riesgos, así como, cuando proceda, acompañada de una evaluación de impacto relativa a la protección de datos conforme al artículo 35 del RGPD, poniendo máximo énfasis 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) Alcance estratégico. La seguridad de la información deberá contar con el compromiso y apoyo de todos los niveles directivos de forma que pueda estar coordinada e integrada con el resto de las iniciativas estratégicas del Departamento para conformar un todo coherente y eficaz.

c) Seguridad Integral. La seguridad constituirá un proceso integral compuesto por todos los elementos técnicos, humanos, materiales y organizativos relacionados con el sistema basado en la mejora continua de todos ellos y del proceso en sí mismo.

d) Análisis y gestión de riesgos: Todos los sistemas afectados por esta PSI, así como todos los tratamientos de datos personales, serán objeto de un análisis de riesgos que evalúe las amenazas y los riesgos a los que están expuestos. Este análisis, que deberá ajustarse, en todo caso, a un criterio de proporcionalidad de los riesgos potenciales y la criticidad y valor de la información y de los servicios afectados, y de acuerdo con los artículos 24, 25, 32 y 35 del RGPD, el artículo 28 de la LOPDGDD y el artículo 3 del ENS cuando el sistema de información trate datos personales, se realizará:

1.º Regularmente, al menos una vez al año, revisando la situación del Sistema de información para determinar si se han producido cambios que requieran una actualización en materia de seguridad.

2.º Cuando cambie la información manejada o los servicios prestados de manera significativa.

3.º Cuando ocurra un incidente grave de seguridad o se detecten vulnerabilidades graves.

e) Prevención, reacción, recuperación y mejora continua. Se implementará un proceso integral de prevención, reacción y recuperación frente a incidentes de seguridad con procedimientos de detección, análisis, comunicación, resolución y registro de las actuaciones para la mejora continua de la seguridad de los sistemas, designando un punto de contacto para las comunicaciones con respecto a incidentes detectados y estableciendo protocolos para el intercambio de información relacionada con el incidente, incluyendo las comunicaciones con los Equipos de Respuesta a Emergencias (CERT) establecidos por el Departamento.

f) Líneas de defensa. Se implementará una estrategia de protección basada en múltiples capas, constituidas por medidas organizativas, físicas y lógicas, de tal forma que cuando una de las capas falla, el sistema implementado permitirá ganar tiempo para una reacción adecuada frente a los incidentes que no han podido evitarse; reducir la probabilidad de que el sistema sea comprometido en su conjunto y minimizar el impacto final sobre el mismo.

cve: BOE-A-2026-13949
Verificable en https://www.boe.es

g) Reevaluación periódica e integridad y actualización del sistema. Se implementarán controles y evaluaciones regulares y periódicas de la seguridad (de forma interna o con la ayuda de terceros) para conocer en todo momento el estado de la seguridad de los sistemas con el objeto de adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección, llegando incluso a un replanteamiento de la seguridad, si fuese necesario.

h) Función diferenciada. El MPTMD organizará su seguridad comprometiendo a todos los miembros del Departamento mediante la designación de diferentes roles de seguridad con responsabilidades claramente diferenciadas, tal y como se recoge en esta orden y se establecerá en el Comité de Seguridad de la información. Los controles establecidos, así como los roles y responsabilidades de seguridad de todo el personal, estarán claramente definidos y documentados.

3. En los supuestos en los que existan tratamientos de datos de carácter personal se identificará al responsable del tratamiento y, en su caso, al encargado del tratamiento, en el Registro de Actividades de Tratamiento, de acuerdo con lo previsto en el artículo 13.2 de esta orden. Dicho registro contendrá toda la información exigida por el artículo 30 del RGPD.

4. Estos principios particulares, en su continuo fortalecimiento y revisión, se ajustarán en todo caso a las instrucciones técnicas de seguridad aprobadas por la persona titular del Ministerio para la Transformación Digital y de la Función Pública de acuerdo con lo previsto en la disposición adicional segunda del ENS, así como a las guías CCN-STIC.

Artículo 6. *Requisitos de Seguridad de la información.*

Tal y como establece el ENS, la política de seguridad debe desarrollarse aplicando una serie de requisitos mínimos cuyo ejercicio corresponderá a los miembros del Departamento establecidos a tal fin, y cuya supervisión realizará el Comité de Seguridad de la información regulado en el artículo 9:

a) Organización e implantación del proceso de seguridad. La seguridad deberá comprometer a todo el personal del MPTMD.

b) Análisis y gestión de los riesgos. Se realizará una gestión de los riesgos consistente en un proceso de identificación, análisis, evaluación y tratamiento a los que el sistema esté expuesto. Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos:

1.º Cuando un sistema de información trate datos personales, la persona responsable o encargada del tratamiento, asesorada por la persona designada como Delegada de Protección de Datos, en adelante DPD, realizará un análisis de riesgos conforme al artículo 24 del RGPD y, en los supuestos de su artículo 35, una evaluación de impacto en la protección de datos.

2.º El análisis y la gestión deberá realizarse de acuerdo con las previsiones del artículo 15 de esta orden, adaptando los criterios de determinación del riesgo en el tratamiento de los datos conforme a lo establecido en el artículo 32 del RGPD y, en caso necesario, estableciendo niveles de seguridad más altos.

c) Gestión de personal y profesionalidad. Se establecerá un programa de concienciación continua anual para formar a todos los empleados públicos que prestan servicio en su ámbito, en particular, a los de nueva incorporación. Del mismo modo, las personas con responsabilidad concreta en el uso, operación o administración de sistemas TIC recibirán formación específica para el manejo seguro de los sistemas en la medida en que la necesitan para realizar su trabajo. La formación será obligatoria antes de asumir una nueva responsabilidad, tanto si es la primera asignación como si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

cve: BOE-A-2026-13949
Verificable en https://www.boe.es

d) Autorización y control de los accesos. Se implementarán mecanismos de control de acceso al sistema general de información, limitándolos a los estrictamente necesarios y debidamente autorizados. Los sistemas de información individuales se diseñarán de forma que garanticen la seguridad por defecto, proporcionando la mínima funcionalidad requerida para alcanzar los objetivos y priorizando el uso sencillo, de tal forma que una utilización insegura requiera, en todo caso, de un acto consciente por parte del usuario. Tales sistemas de información individuales serán solo accesibles por las personas o desde emplazamientos o equipos autorizados, pudiendo exigirse, en su caso, restricciones de horario y puntos de acceso facultados.

e) Protección de las instalaciones. Se implementarán mecanismos de control de acceso físico, previniendo los accesos físicos no autorizados, así como los daños a la información y a los recursos, mediante perímetros de seguridad, controles físicos y protecciones generales en áreas.

f) Adquisición de productos. Ante cualquier adquisición, el MPTMD tendrá en cuenta que dichos productos tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen.

g) Seguridad por defecto. Los sistemas deberán diseñarse y configurarse de forma que garanticen la seguridad por defecto. El sistema proporcionará la mínima funcionalidad requerida para que la organización alcance sus objetivos. Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que solo son accesibles por las personas, o desde emplazamientos o equipos, autorizados.

h) Cuando el sistema trate datos personales, se deberán aplicar medidas de seguridad desde el diseño y por defecto, conforme a lo establecido en los artículos 24 y 25 del RGPD, garantizando que la protección de la información esté incorporada en la arquitectura del sistema y que, por defecto, solo se procesen los datos estrictamente necesarios para la finalidad prevista.

i) Integridad y actualización del sistema. Todo elemento físico o lógico requerirá autorización formal previa a su instalación en el sistema. Se deberá conocer en todo momento el estado de seguridad de los sistemas, en relación con las especificaciones de los fabricantes, las vulnerabilidades y las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de estos.

j) Protección de la información almacenada y en tránsito. Se implementarán mecanismos para proteger la información almacenada o en tránsito, especialmente cuando esta se encuentra en entornos inseguros (portátiles, tablets, soportes de información, redes abiertas, etc.). Los sistemas dispondrán de los medios de protección de la información almacenada y en tránsito (copias de seguridad y otros mecanismos necesarios), que garanticen la continuidad de las operaciones en caso de pérdida de los medios habituales de trabajo.

k) Prevención ante otros sistemas de información interconectados. La estrategia de protección protegerá el perímetro, en particular, si se conecta a redes públicas. En todo caso, analizará los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas y se controlará su punto de unión.

l) Registro de actividad. Se habilitarán registros de la actividad de las personas usuarias reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de las personas afectadas, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral y demás disposiciones que resulten de aplicación.

m) Incidentes de seguridad. Se establecerá un sistema de detección y reacción frente a código dañino.

cve: BOE-A-2026-13949
Verificable en https://www.boe.es

n) La gestión de incidentes que afecten a datos personales tendrá en cuenta lo dispuesto en el RGPD, la LOPDGDD, en especial su disposición adicional primera, así como el resto de la normativa de aplicación.

Se deberán articular medios organizativos y materiales que, en los supuestos de violación de la seguridad de los datos personales, garanticen la notificación a la autoridad de control, la documentación del incidente y la comunicación a los interesados, en su caso, requiriendo para ello la implicación de la persona designada como DPD.

ñ) Continuidad de la actividad. Los sistemas de información del MPTMD dispondrán de copias de seguridad y establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales de trabajo.

o) Mejora continua del proceso de seguridad. El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua.

p) Auditoría de seguridad. Se promoverán las auditorías de los sistemas de información de manera regular, al menos cada dos años, para que se verifique el cumplimiento de los requerimientos del ENS, siguiendo la normativa vigente en función de la categoría de cada sistema de información.

q) Uso de Herramientas de Inteligencia Artificial Generativa Externa. El MPTMD se alinea con las exigencias de las normativas de protección de datos y el marco regulatorio europeo sobre Inteligencia Artificial, promoviendo un uso seguro y ético de la tecnología, de manera que:

1.º Adoptará el principio de prudencia y control estricto sobre el uso de tecnologías y servicios externos, especialmente aquellos emergentes como la Inteligencia Artificial (IA) generativa. En aplicación de este principio, y para salvaguardar la confidencialidad, integridad y disponibilidad de la información bajo su responsabilidad, no se permitirá la transferencia o uso de información del Departamento en plataformas de IA generativa externas que no hayan sido explícitamente evaluadas y autorizadas por los órganos competentes, máxime si tal información permite identificar directa o indirectamente a una persona física, lo cual tiene la naturaleza de dato personal de conformidad con lo establecido en el artículo 4.1) del RGPD.

2.º En el caso de que implique un tratamiento de datos de carácter personal, verificará que se cumple estrictamente con la normativa de protección de datos de carácter personal. Para ello, se comprobará que el tratamiento tenga una base jurídica adecuada conforme al artículo 6.1. del RGPD; que se cumple la obligación de informar de conformidad con los artículos 13 y 14 del RGPD, así como que se adoptan las medidas para garantizar la aplicación efectiva de los principios de protección de datos y la seguridad del tratamiento, la evaluación de impacto y la atención a las solicitudes de derechos del titular de los datos.

3.º En todo caso se estará a disposición de lo indicado por la Agencia Española de Protección de Datos, así como lo dispuesto por la Agencia Española de Supervisión de la Inteligencia Artificial en el desarrollo de tratamientos de datos o sistemas de información que impliquen el uso de inteligencia artificial.

Artículo 7. *Desarrollo de la Política de Seguridad.*

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

a) Primer nivel normativo: constituido por esta PSI y las directrices generales de seguridad aplicables al MPTMD, conforme a lo indicado en el artículo 1.

b) Segundo nivel normativo: constituido por las normas de seguridad desarrolladas por cada órgano superior o directivo del MPTMD o aquellas que se desarrollen para ámbitos o sistemas de información concretos.

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

cve: BOE-A-2026-13949
Verificable en https://www.boe.es

2. Estas normas de seguridad deberán:

a) Aplicarse a los órganos superiores o directivos cuyo ámbito quede determinado por los sistemas de información, los tratamientos de datos personales y servicios de tecnologías de la información y de las comunicaciones a los que da servicio.
b) Cumplir estrictamente con lo indicado en el ENS, con la normativa vigente en materia de protección de datos personales y con los niveles normativos enunciado en este artículo.

3. Además de la normativa enunciada con anterioridad, la estructura normativa podrá disponer, a criterio de cada uno de los órganos directivos a los que se aplica esta PSI, y siempre dentro del ámbito de sus competencias y responsabilidades, de otros documentos tales como: estándares de seguridad, buenas prácticas, informes técnicos, etc.
4. El personal del Departamento tendrá la obligación de conocer y cumplir, además de la presente PSI, todas las directrices generales, normas y procedimientos de seguridad de la información que puedan afectar a sus funciones.

Artículo 8. *Estructura organizativa.*

1. La estructura organizativa para la gestión de la seguridad de la información en el ámbito descrito por la PSI del MPTMD está compuesta por:

a) El Comité de Seguridad de la información.
b) El Responsable o Responsables de la Seguridad de la información.
c) Los Responsables de la información, del servicio y del tratamiento.
d) El Responsable o Responsables del Sistema.
e) Los Responsables y los encargados del tratamiento de datos personales.
f) La persona designada como DPD en el Ministerio.

2. La estructura organizativa será competente para mantener, actualizar y hacer cumplir, dentro del ámbito definido por esta orden, la PSI del MPTMD.

Artículo 9. *Composición y funciones del Comité de Seguridad de la información.*

1. El Comité de Seguridad de la información, órgano colegiado de los previstos en el artículo 22.2 de la Ley 40/2015, de 1 de octubre, adscrito a la Subsecretaría de Política Territorial y Memoria Democrática, estará compuesto por:

a) Presidencia: La persona titular de la División de Tecnologías de la información.
b) Secretaría: La persona, personas u órgano que ocupe el cargo de Responsable de la Seguridad de la información, que ejercerá sus funciones con voz y voto.
c) Vocales:

1.º La persona designada como Responsable del Sistema en cada caso.
2.º Las personas designadas como Responsables de los Servicios.
3.º Las personas designadas como Responsables de la información.
4.º La persona titular de la División de Tecnologías de la Información de la Administración General del Estado en el Territorio.

d) La persona designada como DPD del Departamento, que actuará como asesor con voz, pero sin voto, para garantizar su independencia en atención a la naturaleza de sus funciones de asistencia y apoyo.

cve: BOE-A-2026-13949
Verificable en https://www.boe.es

2. El Comité de Seguridad de la información ejercerá las siguientes funciones en el marco de la PSI:

a) Elaborar las propuestas de modificación y actualización permanente de esta PSI del MPTMD, que se elevarán al titular del Departamento para su aprobación conforme a lo establecido en el artículo 12.3 del ENS.
b) Impulsar el cumplimiento de esta PSI y su desarrollo normativo.
c) Aprobar las normas de desarrollo de esta PSI de segundo nivel.
d) Velar por la difusión de esta PSI, promoviendo actividades de concienciación y formación en materia de seguridad para el personal del Departamento.
e) 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.
f) Tomar aquellas decisiones que garanticen la seguridad de la información y de los servicios del Departamento.
g) Promover la mejora continua en la gestión de la seguridad de la información.
h) Aprobar el Plan de Auditoría y el Plan de Formación propuestos por el Responsable o Responsables de la Seguridad de la información.
i) Resolver los conflictos de competencia que pudieran aparecer entre los diferentes centros directivos en materia de seguridad de la información.
j) Compartir experiencias de éxito en materia de seguridad entre sus miembros para velar por el cumplimiento de esta PSI y su normativa de desarrollo.
k) Definir, dentro del marco establecido por esta orden, la asignación de roles y los criterios para alcanzar las garantías que estime pertinentes en lo relativo a la segregación de tareas.

3. El Comité de Seguridad de la información podrá crear grupos o comités de trabajo con carácter técnico, cuya función será exclusivamente de apoyo y asesoramiento, sin capacidad decisoria. Estos grupos estarán integrados por personal del Departamento y, en su caso, podrán recabar información o asistencia puntual de personal técnico externo para la elaboración de estudios, propuestas de actualización de la PSI, normativa y procedimientos de seguridad, análisis de situación, actividades de formación y concienciación, así como para coordinar la comunicación con el Centro de Operaciones de Seguridad de la Administración General del Estado y, en su caso, con el Centro Criptológico Nacional en la utilización de servicios de respuesta a incidentes de seguridad.
4. El Comité de Seguridad de la información integrará en su composición a los responsables relacionados con los sistemas de información existentes en los servicios territoriales o periféricos ministeriales en aquellas cuestiones que les afecten de forma directa, sin perjuicio de que se constituya un subcomité de seguridad de la información específico para dichos servicios, que integre a los Responsables de la Seguridad de la Información, Responsables de Servicios e Información y Responsables de los Sistemas correspondientes, con las atribuciones y competencias atribuidas al Comité de Seguridad de la Información.
5. En relación con el funcionamiento del Comité, en todo aquello no regulado expresamente en este artículo, será de aplicación lo dispuesto en el título preliminar, capítulo II, sección 3.ª de la Ley 40/2015, de 1 de octubre.

Artículo 10. *El Responsable de la Seguridad de la información.*

1. El Responsable o Responsables de la Seguridad de la información es la persona u órgano que toma las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios. La persona titular de la Subsecretaría de Política Territorial y Memoria Democrática designará la persona u órgano Responsable de la Seguridad de la información.

cve: BOE-A-2026-13949
Verificable en https://www.boe.es

2. Serán funciones de la persona u órgano Responsable de la Seguridad de la información las siguientes:

a) Promover 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.
c) Velar e impulsar el cumplimiento del cuerpo normativo.
d) Encargarse de que la documentación de seguridad se mantenga organizada y actualizada, y de gestionar los mecanismos de acceso a la misma.
e) Promover la mejora continua en la gestión de la seguridad de la información.
f) Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución y participar en la toma de decisiones en momentos de alerta.
g) Impulsar la formación y concienciación en materia de seguridad de la información.
h) Proponer la categoría del sistema según el procedimiento descrito en el ENS y las medidas de seguridad que deben aplicarse de acuerdo con lo previsto en sus anexos I y II.
i) Asumir las funciones explícitamente atribuidas a la persona u órgano Responsable de la Seguridad de la información en el ENS.

Artículo 11. *Los Responsables de la información y los Responsables del servicio.*

1. La persona titular de cada órgano directivo al que den servicio los sistemas a los que se les aplica esta PSI será el Responsable de la información y del servicio. A estos efectos, se entenderá por órganos directivos, conforme a lo dispuesto en la Ley 40/2015, de 1 de octubre, las personas titulares de las Subsecretarías, Secretarías Generales, Secretarías Generales Técnicas, Direcciones Generales y Subdirecciones Generales, así como de las Delegaciones, Subdelegaciones del Gobierno y Direcciones insulares.
2. Coincidirán en una misma figura las responsabilidades de la información y del servicio salvo en aquellos casos en los que el sistema de información maneje información de diferentes órganos directivos o cuando la prestación del servicio no dependa del órgano directivo responsable de la información.
3. Las responsabilidades vinculadas a la PSI y los derivados de la gestión de la seguridad de la información no implicarán, en ningún caso, un aumento de las actuales dotaciones ni de las retribuciones de dichos efectivos.
4. Los Responsables de la información y del servicio tienen la potestad, dentro de su ámbito de actuación y de sus competencias, de establecer los requisitos de seguridad de la información que manejan y de los servicios bajo su competencia y, por tanto, de su protección.
5. Los Responsables de la información tendrán como competencia participar, y en su caso, aceptar los riesgos residuales que afecten a los activos de información bajo su ámbito de actuación, según se indica en el artículo 15, incluyendo aquellos que afecten a datos de carácter personal.
6. Por su parte, los Responsables del servicio, tendrán la competencia de determinar los niveles de seguridad requeridos para el servicio o servicios bajo su ámbito de actuación, estableciendo los requisitos y valoración en términos de criticidad y disponibilidad. Del mismo modo, los Responsables del servicio tendrán la competencia de participar, y en su caso, aceptar los riesgos residuales que afecten a los servicios bajo su ámbito de actuación, según se indica en el artículo 15.
7. Si los servicios y la información manejada incluyen datos de carácter personal, los Responsables de la información y los Responsables del servicio deberán tener en cuenta, además, los requisitos derivados de la legislación correspondiente sobre protección de datos.

cve: BOE-A-2026-13949
Verificable en https://www.boe.es

Artículo 12. *Los Responsables del Sistema.*

1. El Responsable del Sistema es la persona cuya responsabilidad es desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, así como elaborar la normativa de seguridad de tercer nivel definida en esta orden.
2. La persona titular de la dirección de la División de Tecnologías de la Información nombrará a un responsable o responsables del sistema en función de las capacidades sobre el desarrollo, operación y mantenimiento de los sistemas de información en particular.
3. Se prevé expresamente la posibilidad de delegación de las funciones atribuidas al Responsable del sistema. En cualquier caso, el Responsable del sistema actuará como interlocutor entre el responsable de la operación y mantenimiento de sistemas y el Responsable o Responsables de la seguridad de la información del Departamento, así como de interlocutor frente al Comité de Seguridad. En ningún caso la delegación implicará la transferencia de las competencias decisorias que corresponden al Responsable del sistema según lo establecido en la PSI.
4. En cualquier caso, aquellas personas u órganos con responsabilidades sobre los sistemas del Departamento deberán disponer de una persona encargada de verificar el cumplimiento de lo dispuesto en la presente PSI.

Artículo 13. *Los Responsables y encargados del tratamiento de datos personales.*

1. El responsable de tratamiento es quien determina los fines y medios del tratamiento y aplica las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con la normativa vigente en materia de protección de datos personales.
2. La identidad del responsable de tratamiento figura en el registro de las actividades de tratamiento efectuadas bajo su responsabilidad, de acuerdo con lo dispuesto en el artículo 30 del RGPD.
3. El encargado de tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que trata datos personales por cuenta del responsable del tratamiento.

Artículo 14. *La persona designada como Delegada de Protección de Datos (DPD).*

1. La persona designada como DPD, conforme a lo establecido en el artículo 37.5 del RGPD, es designada 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 indicadas en el artículo 39 de dicho reglamento.
2. En el ámbito de los tratamientos de datos de carácter personal, y sin perjuicio de las atribuciones establecidas en el RGPD de forma exclusiva a los responsables y encargados del tratamiento de datos personales, y de las atribuciones exclusivas del Responsable o Responsables de la Seguridad de la información; la persona que tenga las atribuciones de DPD ejercerá labores de asesoramiento y supervisión en orden al cumplimiento de lo establecido en el RGPD, la LOPGDD, así como las guías, directrices e instrucciones de la AEPD y del Comité Europeo de Protección de Datos.
3. Prestará asistencia y asesoramiento a los responsables del tratamiento, a la hora de identificar los riesgos y adoptar medidas para la protección de los datos personales, y en cuanto a la supervisión de que las mismas se han adoptado y llevado a la práctica. En cualquier caso, las funciones ejecutivas de toma de las decisiones oportunas al respecto serán responsabilidad de los respectivos responsables del tratamiento.
4. Ejercerá labores de asistencia y asesoramiento a los responsables del tratamiento de datos personales, a los Responsables de la Seguridad y a los responsables del Sistema, en los procesos de gestión de brechas de datos personales en el ámbito de la gestión general de incidentes de seguridad.

cve: BOE-A-2026-13949
Verificable en https://www.boe.es

5. Prestará asesoramiento a los Responsables de la Seguridad y a los Responsables del Sistema, en cuanto a la implantación de medidas de seguridad que tengan un objeto distinto que la protección de datos, en la medida en que impliquen un tratamiento adicional de datos personales, tal y como dispone el artículo 24 del ENS.

6. Conforme a lo establecido en el artículo 38.3 RGPD, el responsable y el encargado del tratamiento garantizarán que el DPD no reciba ninguna instrucción en lo que respecta al desempeño de sus funciones. No será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones, y rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado.

Artículo 15. *Resolución de conflictos.*

En caso de conflicto entre los diferentes responsables que componen la estructura organizativa de esta PSI prevalecerá la decisión del Comité de Seguridad de la información.

Artículo 16. *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 basada en los riesgos y reevaluación periódica.

2. El Responsable del servicio es el encargado de que se realice el preceptivo análisis de riesgos y se proponga el tratamiento adecuado, calculando los riesgos residuales.

3. El Responsable o Responsables de la Seguridad de la información, dentro de su ámbito de actuación, es la persona u órgano encargado de recomendar un marco de directrices básicas para armonizar los criterios a seguir para la valoración de riesgos.

4. Los Responsables de la información y del servicio son quienes gestionan y asumen 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.

5. 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 directivo, a través de un Plan de Adecuación al ENS:

a) Las indicadas fases del proceso de gestión de riesgos se realizarán según lo dispuesto en el capítulo III del ENS y siguiendo las normas, instrucciones, guías CCN-STIC y recomendaciones para la aplicación de este 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 RGPD.

b) En el caso de que existan tratamientos de datos personales, se deberá tener en cuenta lo dispuesto en el artículo 17, de modo que los requisitos identificados conforme a dicho artículo y, con el asesoramiento específico del DPD, se puedan añadir a los establecidos conforme al ENS si así fuera necesario, en particular, fijando el nivel de seguridad a un nivel más alto. En estos casos, si el resultado del análisis es que los tratamientos de datos personales fuesen de alto riesgo, estos requisitos se elaborarán con la formalidad de una evaluación de impacto en la protección de datos, conforme al artículo 35 del RGPD y los criterios establecidos por la Agencia Española de Protección de Datos. En este aspecto, también se deberá tener en cuenta la regulación de la seguridad de los tratamientos de datos personales, especificada en el artículo 32 del RGPD. En caso de que se produzca una violación de seguridad de los datos personales, se procederá conforme a lo previsto en los artículos 33 y 34 del RGPD.

cve: BOE-A-2026-13949
Verificable en https://www.boe.es

Artículo 17. *Protección de Datos de Carácter Personal.*

Se aplicarán a los datos de carácter personal que sean objeto de tratamiento por parte del MPTMD, las medidas de seguridad apropiadas derivadas del análisis de riesgos, así como de la evaluación de impacto relativa a la protección de datos, que se detalla en el RGPD y en la LOPDGDD:

a) Se aplicarán las medidas correspondientes al anexo II del ENS. En el caso de que el análisis de riesgos determine medidas agravadas respecto a las citadas en dicho anexo, éstas serán las que se implementarán en la protección de datos de carácter personal. En particular, se tendrá en cuenta el artículo 32 del RGPD, en cuanto a la exigencia de una identificación de riesgos específicos para los derechos y libertades de las personas en relación con los tratamientos de datos personales, que debe ser previo al análisis de riesgos de los sistemas donde se implementen dichos tratamientos, de forma que el nivel de seguridad sea adecuado al riesgo que los tratamientos de datos personales suponen para los derechos y libertades de las personas.

b) Los servicios de ciberseguridad y administración de sistemas, dependientes de los respectivos Responsables de los Sistemas, podrán implementar tratamientos de datos personales que se atendrán al tratamiento estrictamente necesario y proporcionado a la finalidad perseguida como consecuencia de la implantación de medidas de seguridad que tengan un objeto distinto de la protección de datos personales, en base a lo dispuesto en el artículo 24 del ENS.

c) Con objeto de preservar la seguridad de los sistemas de información, garantizando la rigurosa observancia de los principios de actuación de las Administraciones públicas, y de conformidad con lo dispuesto en el RGPD y el respeto a los principios de limitación de la finalidad, minimización de los datos y limitación del plazo de conservación allí enunciados, se podrá, en la medida estrictamente necesaria y proporcionada a la finalidad perseguida, analizar las comunicaciones entrantes o salientes, y únicamente para los fines de seguridad de la información, de forma que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la distribución malintencionada de código dañino así como otros daños a las antedichas redes y sistemas de información al tenor de lo dispuesto en el apartado 24.2 del ENS.

Artículo 18. *Formación y concienciación.*

1. Se desarrollarán actividades de formación y concienciación específicas dirigidas al personal empleado público del MPTMD, al de nueva incorporación o al que es objeto de cambio de puesto, así como a la difusión de esta PSI y de su desarrollo normativo.

2. El Comité de Seguridad, y los Responsables de seguridad, serán los responsables de promover las actividades, según lo indicado en esta orden.

Disposición adicional primera. *Servicios territoriales no integrados.*

En aplicación de lo dispuesto en el artículo 71.3 de la Ley 40/2015, de 1 de octubre, los órganos territoriales responsables de los servicios territoriales no integrados aplicarán la PSI aprobada por el órgano central competente sobre el sector de actividad en el que ellos operen.

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

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

cve: BOE-A-2026-13949
Verificable en https://www.boe.es

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 adicional cuarta. *Publicación en la sede electrónica asociada del MPTMD.*

Sin perjuicio de lo previsto en la disposición final única, la PSI aprobada mediante esta orden se publicará también en la sede electrónica asociada del MPTMD.

Disposición derogatoria única. *Derogación normativa.*

Quedan derogadas las disposiciones de igual o inferior rango en lo que se opongan a lo dispuesto en esta orden ministerial y, en particular, la Orden TAP/3148/2011, de 7 de octubre, por la que se aprueba la política de seguridad de la información en el ámbito de la administración electrónica del Ministerio de Política Territorial y Administración Pública.

Disposición final única. *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 junio de 2026.–El Ministro de Política Territorial y Memoria Democrática, Ángel Víctor Torres Pérez.

cve: BOE-A-2026-13949
Verificable en https://www.boe.es