III. OTRAS DISPOSICIONES

MINISTERIO DE INDUSTRIA Y TURISMO

21533 *Orden ITU/1176/2025, de 17 de octubre, por la que se aprueba la Política de Seguridad de la Información del Ministerio de Industria y Turismo.*

El marco normativo que ampara la relación entre la Administración Pública y la ciudadanía a través de los medios electrónicos se encuentra establecido en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Ambas normas han sido desarrolladas 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, que persigue cuatro grandes objetivos: mejorar la eficiencia administrativa, incrementar la transparencia y la participación, garantizar servicios digitales fácilmente utilizables y mejorar la seguridad jurídica.

En consonancia con ello y para contribuir al rápido desarrollo de la sociedad de la información es indispensable trabajar por el fomento de un clima de confianza, que garantice la seguridad de la información, las infraestructuras de red, la autenticación, la privacidad y la protección de las personas consumidoras y usuarias de tecnologías de la información.

Estas previsiones se plasman en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, y cuyo objeto es establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de las relaciones entre la Administración Pública y la ciudadanía a través de los medios electrónicos, estableciendo los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada y los servicios prestados.

De igual forma, 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, el 27 de diciembre de 2022, se publicó la 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 con el objetivo de mejorar el funcionamiento del mercado interior. Esta Directiva 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.

Asimismo, 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 por el que se deroga la Directiva 95/46/CE (en adelante RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, introducen un nuevo conjunto de medidas destinadas a aumentar la confianza en el tratamiento de datos, amparando así un derecho fundamental protegido por el artículo 18.4 de la Constitución Española.

Finalmente, y cumpliendo con el mandato recogido en el artículo 12 del Real Decreto 311/2022, de 3 de mayo, se dicta la presente orden, que atiende a la necesidad

cve: BOE-A-2025-21533
Verificable en https://www.boe.es

de aprobar la Política de Seguridad de la Información del Departamento. Además, en la elaboración de la misma, se han cumplido los principios de buena regulación establecidos en el artículo 129 de la Ley 39/2015, de 1 de octubre. Consuma los principios de necesidad y eficacia, pues se trata del instrumento óptimo para garantizar una Política de Seguridad en la utilización de medios electrónicos que permita una adecuada protección de la información dentro del Departamento. Se adecua al principio de proporcionalidad, ya que no existe otra alternativa menos restrictiva de derechos o que imponga más obligaciones y, en cuanto a los principios de seguridad jurídica, transparencia y eficiencia, la norma es coherente con el resto del ordenamiento jurídico y se ha procurado la participación de las partes interesadas, permitiendo una gestión más eficiente de los recursos públicos y no contempla cargas administrativas.

Esta norma es de carácter únicamente organizativo y, por ello se pueden omitir los trámites de consulta pública previa, audiencia e información públicas.

Se ha recabado informe de la Secretaría General Técnica del Departamento, de la Agencia Estatal de Administración Digital y de la Agencia Española de Protección de Datos.

En virtud de lo anterior, y 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 al ámbito de la Administración Electrónica, constituye el objeto de la presente orden la aprobación de la Política de Seguridad de la Información (en adelante PSI) en el ámbito de la Administración Digital del Ministerio de Industria y Turismo, así como la regulación de su marco organizativo y sus funciones.

2. La PSI será de obligado cumplimiento para todos los órganos del Ministerio de Industria y Turismo, así como para los organismos y entidades vinculados o dependientes de los mismos, que no tengan establecida su propia política de seguridad de la información. En aquellos organismos que tengan su propia política de seguridad de la información prevalecerá, en caso de discrepancia, la definida en esta orden ministerial.

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

Artículo 2. *Misión del Departamento.*

El Ministerio de Industria y Turismo, de acuerdo con lo establecido en el Real Decreto 409/2024, de 23 de abril por el que se desarrolla la estructura orgánica básica del Ministerio de Industria y Turismo, es el Departamento de la Administración General del Estado encargado de la propuesta y ejecución de la política del Gobierno en materia de industria y turismo que abarca, entre otros aspectos, la estrategia y el desarrollo industrial, del emprendimiento y de la pequeña y mediana empresa; la promoción y defensa de la propiedad industrial y la política de turismo, así como el resto de competencias y atribuciones que le confiere el ordenamiento jurídico.

Artículo 3. *Marco normativo.*

El marco normativo en que se desarrollan las actividades del Ministerio de Industria y Turismo, en el ámbito de la prestación de servicios electrónicos a los ciudadanos, sin perjuicio de la legislación específica, se compone, principalmente, de las siguientes normas:

a) 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

cve: BOE-A-2025-21533
Verificable en https://www.boe.es

deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos), (en adelante RGPD).

b) 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.

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

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

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

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

g) 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.

h) 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.

i) 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 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.

j) El 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) El Real Decreto 409/2024, de 23 de abril, por el que se desarrolla la estructura orgánica básica del Ministerio de Industria y Turismo.

l) 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.

m) La Orden ICT/1078/2019, de 21 de octubre, por la que se regula la protección de la información clasificada en el Ministerio de Industria, Comercio y Turismo.

n) La Orden Comunicada de febrero de 2019 de creación de la Célula de Crisis.

o) La Orden ITU/461/2025, de 8 de mayo, por la que se crea y regula la Comisión Ministerial de Administración Digital del Ministerio de Industria y Turismo.

p) Las normas aplicables a la Administración Electrónica y seguridad de la información que complementen, desarrollen o sustituyan a las anteriores, así como aquellas normas aplicables y de inferior rango que las citadas anteriormente, publicadas en las sedes electrónicas asociadas comprendidas en el ámbito de actuación del Ministerio.

Artículo 4. *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 (en adelante ENS) 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 5. *Estructura organizativa.*

La estructura organizativa para la gestión de la seguridad de la información en el ámbito del Ministerio de Industria y Turismo está compuesta por los siguientes agentes:

a) La Comisión Ministerial de Administración Digital (en adelante CMAD).

b) El Grupo Técnico de Seguridad de la Información (en adelante GTSI).

c) Las personas designadas como Responsables de la Información y Responsables de los Servicios.

d) Las personas designadas como Responsables de la Seguridad.

cve: BOE-A-2025-21533
Verificable en https://www.boe.es

e) Las personas designadas como Responsables de los Sistemas.

f) Las personas designadas como Delegado de Protección de Datos y Delegados de Protección de Datos de los organismos públicos adscritos al Departamento.

g) Las personas designadas como Administradores de Seguridad.

h) Los Jefes de Seguridad de Órganos de Control de los Servicios de Protección de la Información Clasificada.

i) La Célula Ministerial de Crisis.

j) El Servicio Central de Protección de la Información y el Subregistro Principal OTAN/UE.

Artículo 6. *Comisión Ministerial de Administración Digital.*

Como órgano colegiado responsable del impulso y coordinación en materia de Administración Digital, y además de las funciones encomendadas a este órgano en la Orden ITU/461/2025, de 8 de mayo, el Pleno de la misma desempeñará las siguientes funciones en materia de Seguridad de la Información:

a) Establecer, gestionar, coordinar y supervisar la estrategia en materia de seguridad de la información y el cumplimiento del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

b) Coordinar todas las actividades relacionadas con las estrategias de seguridad de los servicios prestados por el Departamento, tanto de carácter horizontal, común o compartido, como de carácter sectorial y promover la mejora continua en la gestión de la seguridad de la información.

c) Resolver los posibles conflictos que puedan derivarse del establecimiento de la estructura organizativa de la presente Política de Seguridad de la Información en el Departamento.

d) Impulsar la adecuación a la normativa aplicable de seguridad de la información y de protección de datos.

e) Proponer la modificación, actualización, evaluación, control, coordinación e interpretación de la PSI, cuya ulterior aprobación corresponde al titular del Departamento. Le compete además proponer la aprobación de la normativa de seguridad de segundo nivel descrita en el artículo 17.

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

1. De acuerdo con el artículo 22.3 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en el seno de la CMAD existirá un grupo de trabajo permanente, denominado Grupo Técnico de Seguridad de la Información (en adelante, GTSI), competente para conocer las cuestiones técnicas que deban abordarse en relación con la PSI y que representa a los órganos con competencias en materia de gestión de tecnologías de la información.

2. El GTSI estará compuesto por los siguientes miembros:

a) Presidente: Persona titular de la Subdirección General de Tecnologías de la Información y las Comunicaciones, dependiente de la Subsecretaría de Industria y Turismo.

b) Responsables de la Seguridad, de acuerdo con la definición del artículo 9.

c) Secretario: Responsable de la Seguridad de la Subdirección General de Tecnologías de la Información y las Comunicaciones, dependiente de la Subsecretaría de Industria y Turismo, que actuará con voz y voto.

En las reuniones del GTSI podrán participar cuantos expertos y asesores, internos o externos, estimen necesarios los miembros del mismo, que tendrán voz, pero no voto en las deliberaciones.

cve: BOE-A-2025-21533
Verificable en https://www.boe.es

3. Las funciones del GTSI serán las siguientes:

a) Elaborar estudios, análisis y propuestas de modificación y actualización de la Política de Seguridad de la Información, de la estrategia de evolución del Departamento en el ámbito de la seguridad de la información y de la normativa de seguridad de la información de segundo nivel.

b) Velar por la coherencia y armonización de la normativa y actuaciones en materia de seguridad de la información entre los distintos servicios ofrecidos por los órganos del Departamento, ya sean los de carácter común, horizontal o sectorial.

c) Estudiar y proponer actividades de concienciación y formación en materia de seguridad de la información, velar e impulsar el cumplimiento del cuerpo normativo a que se refiere el artículo 17, e impulsar y promover la formación y concienciación en materia de seguridad de la información.

d) Realizar cualquier otra actividad de asesoría, formulación de recomendaciones, mejoras o propuesta de iniciativas, en materia de seguridad de la información.

e) 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.

f) Informar periódicamente al titular de la Subsecretaría del Departamento sobre el estado de la seguridad en el ámbito de la PSI. Para ello, podrá utilizar informes de incidentes de seguridad de la información, resultados de auditorías y análisis de riesgos realizados y, en general, cualquier información de seguridad relevante que pueda recabar en el desarrollo de sus funciones.

g) Cualquier otra función en el ámbito de la seguridad de la información y los servicios que le sea encomendada a través de la normativa de seguridad de la información de segundo nivel al respecto.

Artículo 8. *Responsables de la Información y Responsables de los Servicios.*

1. Las personas designadas Responsables de la Información y las personas designadas Responsables de los Servicios, de acuerdo con lo previsto en el artículo 13 del Real Decreto 311/2022, de 3 de mayo, tienen la potestad respectivamente, dentro de su ámbito de actuación y competencias, de aprobar los requisitos en materia de seguridad tanto de la información que manejan como de los servicios que prestan y, por tanto, de su protección. Si esta información incluye datos de carácter personal, además deberán tenerse en cuenta los requisitos derivados de la legislación correspondiente sobre protección de datos.

2. Existirá al menos un Responsable de la Información y un Responsable del Servicio en la Secretaría de Estado de Industria, la Secretaría de Estado de Turismo y en la Subsecretaría, así como en cada organismo o entidad de derecho público vinculado o dependiente del Departamento a los que, conforme al artículo 1, les sea de aplicación la presente Política de Seguridad de la Información. Estos responsables se designarán entre los funcionarios de carrera de nivel 26 o superior, de acuerdo con la organización interna del órgano respectivo, sin que, implique, en ningún caso, un aumento de las actuales dotaciones o retribuciones de dichos efectivos por ningún concepto.

3. Es posible unificar ambas responsabilidades en una sola persona, y su designación corresponderá a la persona titular del órgano superior o directivo correspondiente, y de cada organismo o entidad de derecho público dependiente del Ministerio a los que sea de aplicación esta PSI de acuerdo con su propia organización interna.

4. Serán funciones de las personas designadas Responsables de la Información y Responsables de los Servicios, dentro de sus ámbitos de actuación, las siguientes:

a) Determinar los niveles de seguridad de la información tratada y de los servicios prestados valorando los impactos de los incidentes que afecten a la seguridad de la información y a la seguridad del servicio.

cve: BOE-A-2025-21533
Verificable en https://www.boe.es

b) Realizar los preceptivos análisis de riesgos y seleccionar las salvaguardas que se han de implantar, con la participación de la persona designada Responsable de la Seguridad.

c) Aceptar los riesgos residuales respecto de la información y de los servicios, calculados en el análisis de riesgos.

d) Velar por la no comisión de errores o negligencias que lleven a un incidente de confidencialidad o de integridad de la información tratada.

e) Garantizar el mantenimiento y protección del uso y acceso que se haga de la información de la que son responsables.

f) Cualquier otra función en el ámbito de la seguridad de la información que le sea encomendada a través de la normativa de seguridad de la información de segundo nivel, especificada en el artículo 17.

Artículo 9. *Responsables de la Seguridad.*

1. Las personas designadas Responsables de la Seguridad acuerdan las decisiones necesarias para satisfacer los requisitos de seguridad de la información y de los servicios y supervisan la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos.

2. Existirá un Responsable de la Seguridad en cada órgano superior o directivo del Ministerio con competencias de gestión de tecnologías de la información, así como cada organismo o entidad de derecho público vinculado o dependiente del Departamento a los que les sea de aplicación la presente PSI. Estos responsables se designarán entre los funcionarios de carrera de nivel 26 o superior, de acuerdo con la organización interna del órgano respectivo, sin que implique, en ningún caso, un aumento de las actuales dotaciones ni de las retribuciones de dichos efectivos por ningún concepto.

3. El ámbito de actuación de las personas designadas Responsables de la Seguridad se limita a todos los servicios de tecnologías de la información y las comunicaciones prestados o gestionados directamente por el centro o centros para los que haya sido designado Responsable de la Seguridad, debiendo además velar por la coherencia y armonización de las normas, procedimientos y actuaciones en los diferentes ámbitos.

4. En concreto, le corresponde el desempeño de las siguientes funciones:

a) Elaborar la normativa de seguridad de la información de segundo nivel, definida en el artículo 17, así como aprobar los procedimientos, guías, e instrucciones técnicas vinculadas al tercer nivel normativo, previo acuerdo en el GTSI.

b) Mantener la documentación de seguridad de la información actualizada y organizada, así como gestionar los mecanismos de acceso a esta.

c) Verificar que las medidas de seguridad de la información son adecuadas para la protección de la información y los servicios y proponer las decisiones respecto a las medidas de que considere imprescindibles para preservar la seguridad, integridad y disponibilidad de los servicios prestados y la información manejada por el Departamento.

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

e) Ampliar los requisitos mínimos y adoptar medidas adicionales y compensatorias en relación con las medidas de seguridad de la información, según establece el artículo 28 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

f) Analizar los informes de auditoría de la seguridad de la información y presentar conclusiones al Responsable del Sistema para la adopción las medidas correctoras adecuadas, tal y como regula el artículo 31.5 del Real Decreto 311/2022, de 3 de mayo.

g) Dar publicidad, en los correspondientes portales de internet o sedes electrónicas a las declaraciones y certificaciones de conformidad con el ENS, atendiendo a lo

cve: BOE-A-2025-21533
Verificable en https://www.boe.es

dispuesto en la Instrucción Técnica de Seguridad de la Información, según los términos establecidos en el artículo 38.2 del Real Decreto 311/2022, de 3 de mayo.

h) Cualquier otra función en el ámbito de la seguridad de la información y los servicios que le sea encomendada a través de la normativa de seguridad de la información de segundo nivel al respecto.

5. Las personas designadas Responsable de la Seguridad no podrán ser designadas como Responsable de la Información, ni de los Servicios. Adicionalmente, deberán ser distintas del Responsable de los Sistemas y no podrá existir dependencia jerárquica entre ambos. En aquellas situaciones excepcionales en las que la ausencia justificada de recursos haga necesario que el Responsable de la Seguridad y el Responsable de los Sistemas recaiga en la misma persona, o en distintas personas entre las que exista relación jerárquica, deberán aplicarse 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.

6. En aquellos sistemas de información que, por su complejidad, distribución, separación física de sus elementos o número de usuarios, se necesite de personal adicional para llevar a cabo las funciones de Responsable de la Seguridad, se podrán designar Responsables de la Seguridad Delegados. La designación corresponderá al Responsable de la Seguridad, que delegará funciones, no responsabilidad. Los Responsables de la Seguridad Delegados se harán cargo de todas aquellas funciones encomendadas por el Responsable de la Seguridad. Cada Responsable de la Seguridad Delegado mantendrá una dependencia funcional directa del Responsable de la Seguridad, a quien reportará.

Artículo 10. *Responsables de los Sistemas.*

1. Las personas designadas Responsable de los Sistemas son las encargadas de la explotación de los sistemas de información, así como de desarrollar la forma concreta de implementar la seguridad de la información en los mismos y de la supervisión de la operación diaria de estos. Este ámbito vendrá determinado por los sistemas de información, los tratamientos de datos personales y servicios de tecnologías de la información y de las comunicaciones que sean prestados o gestionados directamente por el centro o centros para los que haya sido designado Responsable de los Sistemas.

2. Cada órgano con competencias de gestión de tecnologías de la información designará un Responsable de los Sistemas entre los funcionarios de carrera de nivel 26 o superior, destinados en el mismo. Cuando la complejidad, distribución, separación física de sus elementos o número de usuarios de los sistemas de información lo justifiquen, el titular del órgano directivo podrá designar los Responsables de Sistema delegados que considere necesarios entre los funcionarios de carrera del órgano directivo, que tendrán dependencia funcional directa del Responsable de los Sistemas y serán responsables en su ámbito de todas aquellas acciones que les delegue. Estos responsables se designarán de acuerdo con la organización interna del órgano respectivo, sin que implique, en ningún caso, un aumento de las actuales dotaciones ni de las retribuciones de dichos efectivos por ningún concepto.

3. Las funciones que le corresponden, en su ámbito de actuación, son:

a) Definir la tipología y sistema de gestión del Sistema de Información, estableciendo los criterios de uso y los servicios disponibles en este.

b) Cerciorarse de que las medidas específicas de seguridad de la información se integren adecuadamente dentro del marco tecnológico y de seguridad del Departamento.

c) Suspender temporalmente el tratamiento de informaciones, la prestación de servicios electrónicos o la total operación del sistema, en el caso de los sistemas de categoría alta, visto el dictamen de auditoría y atendiendo a una eventual gravedad de las deficiencias encontradas, hasta su adecuada subsanación o mitigación.

cve: BOE-A-2025-21533
Verificable en https://www.boe.es

d) Recibir los informes de auditoría de seguridad de la información tal y como establece el artículo 31.5 del Real Decreto 311/2022, de 3 de mayo.

e) Dar publicidad, en los correspondientes portales de internet o sedes electrónicas a las declaraciones y certificaciones de conformidad con el ENS, atendiendo a lo dispuesto en la Instrucción Técnica de Seguridad de la Información, según los términos establecidos en el artículo 38.2 del Real Decreto 311/2022, de 3 de mayo.

f) Cualquier otra función en el ámbito de la seguridad de los sistemas de información que le sea encomendada a través de la normativa de seguridad de segundo nivel al respecto.

4. La persona designada Responsable de los Sistemas podrá nombrar motivadamente, siendo responsable de su actuación, a las personas delegadas como Administradores de los Sistemas que considere necesarios para el adecuado cumplimiento de sus funciones, quienes actuarán bajo su coordinación y de acuerdo con sus criterios.

Artículo 11. *Comunicación de los nombramientos.*

Los nombramientos de las personas designadas Responsables de la Información, Responsables de los Servicios, Responsable de la Seguridad y Responsable de los Sistemas, serán comunicados a la CMAD.

Artículo 12. *Delegado de Protección de Datos.*

1. En el ámbito del tratamiento de datos personales, y sin perjuicio de las atribuciones establecidas en el RGPD de forma exclusiva a los responsables y encargados de los tratamientos de datos personales, y de las atribuciones exclusivas de los Responsables de la Seguridad, el Delegado de Protección de Datos ejercerá labores de asesoramiento y supervisión en el ámbito de la presente norma.

2. El Delegado de Protección de Datos 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.

3. 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 de la información.

4. Prestará asesoramiento a los Responsables de la Seguridad y a los Responsables del Sistema, en cuanto a la implantación de medidas de seguridad de la información que tengan un objeto distinto que la protección de datos, en la medida en que impliquen un tratamiento adicional de datos personales, tal y como dispone el artículo 24 del Real Decreto 311/2022, de 3 de mayo.

Artículo 13. *Servicios de Protección de la Información Clasificada.*

1. Los Servicios de Protección de la información Clasificada del Ministerio de Industria y Turismo se componen de los diversos órganos de control estructurados en dependencia funcional del Servicio Central de Protección de la Información Clasificada/ Subregistro Principal OTAN/UE, bajo la autoridad de su Director, el Subsecretario del Ministerio de Industria y Turismo:

a) Servicio Central de Protección de la Información Clasificada/Subregistro Principal OTAN/UE.

b) Servicios Locales de Protección de la Información Clasificada.

c) Puntos de Control.

cve: BOE-A-2025-21533
Verificable en https://www.boe.es

2. Los órganos de control, por razones de competencia funcional, son responsables superiores del cumplimiento de todos los aspectos referidos a la seguridad de la información clasificada y a la gestión de sus riesgos, independientemente de su formato o modo de transmisión, tanto de su manejo y custodia, de la seguridad física de las instalaciones, seguridad en el personal para su tratamiento, y seguridad en los sistemas de información y comunicaciones.

3. En el ejercicio de sus funciones, llevarán a cabo labores de apoyo y asesoramiento a los distintos responsables de información y de seguridad en cuanto sea requerido y, muy en particular, en aquellos ámbitos en los que sea preciso el manejo de la información clasificada, en cuyo ejercicio velará por establecer la adecuada viabilidad y compatibilidad de las medidas establecidas en aplicación de esta ley.

4. Ejercerán la necesaria coordinación y supervisión en materia de seguridad en los sistemas de información y comunicaciones en relación con el mantenimiento y la implementación de medidas de carácter tecnológico que permitan el manejo seguro de la información clasificada a través de medios digitales en zonas de acceso restringidas o en zonas administrativas de protección.

Artículo 14. *Célula Ministerial de Crisis.*

1. La Célula Ministerial de Crisis, regulada según la Orden comunicada relativa en materia de seguridad nacional en el Ministerio de Industria, Comercio y Turismo de 7 de febrero de 2020, se define como puesto de control y seguimiento de las situaciones de crisis para facilitar el ejercicio de las funciones de Seguridad Nacional en el ámbito de actuación del Ministerio.

2. La Célula Ministerial de Crisis estará presidida por el Subsecretario del Ministerio de Industria y Turismo. Actuará como vicepresidente la persona titular del Gabinete del Ministro en su condición de Punto de Contacto del Departamento en el Sistema de Seguridad Nacional. A sus reuniones podrán asistir aquellos directivos y técnicos que se estime oportuno por razón del asunto a tratar.

3. La Célula Ministerial de Crisis dirigirá y coordinará las actuaciones de gestión en situaciones de crisis, promoviendo la necesaria colaboración entre los Departamentos afectados, a cuyo efecto analiza los escenarios de crisis, y apoya y propone planes de respuesta en coordinación con los órganos competentes del Departamento, en términos que garanticen en todo momento la seguridad de la información según lo establecido en esta ley.

Artículo 15. *Administradores de la Seguridad.*

1. Las personas designadas Administradores de la Seguridad, serán nombradas por el Responsable de la Seguridad, de acuerdo con lo previsto en el artículo 13 del Real Decreto 311/2022, de 3 de mayo, y son responsables de la implementación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema de Información y de la aplicación de los Procedimientos Operativos de Seguridad (POS).

2. Son funciones de las personas designadas Administradores de Seguridad:

a) Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.

b) Gestionar, configurar y actualizar, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del sistema de información.

c) Gestionar las autorizaciones y privilegios concedidos a los usuarios del sistema, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.

d) Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

cve: BOE-A-2025-21533
Verificable en https://www.boe.es

e) Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.

f) Informar al Responsable de la Seguridad de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad de la información.

g) Cualquier otra función en el ámbito de la administración de seguridad de la información que le sea encomendada a través de la normativa de seguridad de la información de segundo nivel al respecto.

3. Las personas designadas Administradores de los Sistemas tendrán dependencia funcional directa del Responsable de la Seguridad.

Artículo 16. *Gestión de los riesgos.*

1. La gestión de riesgos debe realizarse de manera continua sobre los sistemas de información y contemplar un análisis de riesgos avanzado que evalúe los riesgos residuales y proponga tratamientos adecuados. Cuando el análisis de riesgos se aplique a tratamientos de datos personales, se tendrán en cuenta los riesgos posibles que afecten a los derechos y libertades de las personas físicas.

2. Cada órgano superior o directivo del Ministerio, así como cada organismo o entidad de derecho público vinculado o dependiente del Departamento a los que les sea de aplicación la presente Política de Seguridad de la Información, siempre dentro de su ámbito de actuación y de sus competencias, se encargará de analizar y evaluar los riesgos de funcionamiento de los servicios a fin de establecer las correspondientes medidas preventivas.

3. Para la realización del análisis de riesgos se tendrán en cuenta las recomendaciones publicadas para el ámbito de la Administración Pública y, en especial, las guías elaboradas por el Centro Criptológico Nacional, y la Agencia Española de Protección de Datos, y el artículo 14 del Real Decreto 311/2022, de 3 de mayo.

Artículo 17. *Estructuración, gestión y acceso de la documentación de Seguridad de la Información.*

1. Las normas y documentación sobre seguridad de la información en la Administración Electrónica del Departamento se clasificarán jerárquicamente en tres niveles, según su ámbito de aplicación y grado de detalle técnico, de modo que todas se basarán en otra, u otras, de nivel superior.

a) Primer nivel normativo: 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 a los a los que, conforme al artículo 1, sea de aplicación la presente Política de Seguridad de la Información.

b) Segundo nivel normativo: Normativa y recomendaciones de seguridad de la información. 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 u organismos públicos 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 los titulares de los órganos superiores o directivos 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 el GTSI.

c) Tercer nivel normativo: Procesos y Procedimientos Técnicos. Corresponden al desarrollo del segundo nivel normativo y está constituido por Procesos y Procedimientos

cve: BOE-A-2025-21533
Verificable en https://www.boe.es

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 incluyen en este nivel normativo las normas, instrucciones, guías y recomendaciones desarrolladas por el Centro Criptológico Nacional con el fin de mejorar el grado de ciberseguridad de las organizaciones.

2. El GTSI establecerá mecanismos para la gestión de la documentación derivada del desarrollo normativo de la PSI y su acceso, con objeto de estandarizar en la medida de lo posible dicho desarrollo en su ámbito de aplicación teniendo en cuenta los principios de mínimo privilegio y de necesidad de conocer y responsabilidad de compartir.

Artículo 18. *Protección de datos de carácter personal.*

1. El tratamiento de datos de carácter personal en el ámbito del Ministerio de Industria y Turismo 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 Industria y Turismo, además de sus 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).

3. En caso de conflicto con la normativa de seguridad de la información indicada en el artículo 17 prevalecerá la norma que presente un mayor nivel de exigencia respecto a la protección de los datos personales, según el criterio del Delegado de Protección de Datos.

4. 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 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.

Artículo 19. *Formación y concienciación.*

Se llevarán a cabo actividades formativas específicas orientadas a la concienciación y formación de los empleados públicos del Departamento en el ámbito de la seguridad de la información, así como a la difusión entre ellos de la PSI y de su desarrollo normativo. A estos efectos, deberán incluirse actividades formativas en esta materia dentro de los planes de formación del Ministerio.

cve: BOE-A-2025-21533
Verificable en https://www.boe.es

Artículo 20. *Actualización permanente y revisiones.*

1. La Política de Seguridad de la Información deberá actualizarse permanentemente para adecuarla al progreso de los servicios de Administración Electrónica, la evolución tecnológica, el desarrollo de la sociedad de la información, y los estándares internacionales de seguridad de la información.

2. Las propuestas de las sucesivas revisiones de la PSI se elaborarán por el GTSI, con conocimiento del Delegado de Protección de Datos y del Jefe de Seguridad del Servicio Central de Protección de la Información Clasificada, y serán aprobadas por la CMAD.

Disposición adicional primera. *Política de seguridad de la información de los organismos y entidades vinculados, dependientes o adscritos al Ministerio de Industria y Turismo.*

1. De acuerdo con lo previsto en el artículo 12.3 del Real Decreto 311/2022, de 3 de mayo, y el artículo 1.2 de esta orden, los organismos y entidades vinculados, dependientes o adscritos al Ministerio de Industria y Turismo 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.

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

La aplicación de esta orden no conllevará incremento de 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 esta orden y, en particular, la Orden IET/1934/2014, de 14 de octubre, por la que se establece la política de seguridad de la información en el ámbito de la administración electrónica del Ministerio de Industria, Energía y Turismo.

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, 17 de octubre de 2025.–El Ministro de Industria y Turismo, Jordi Hereu Boher.

cve: BOE-A-2025-21533
Verificable en https://www.boe.es