Orden TEC/469/2019, de 15 de abril, por la que se aprueba la Política de Seguridad de la Información en el ámbito de la administración electrónica y se crea la Comisión Ministerial de Administración Digital del Ministerio para la Transición Ecológica.

Ministerio para la Transición Ecológica
«BOE» núm. 100, de 26 de abril de 2019
Referencia: BOE-A-2019-6203

TEXTO CONSOLIDADO
Última modificación: sin modificaciones

La Ley 39/2015 de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, recoge en el artículo 13 relativo a los derechos de las personas en sus relaciones con las Administraciones Públicas, en su letra h), el derecho «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 otro lado, en su artículo 17.3, sobre el archivo de documentos, se indica que «Los medios o soportes en que se almacenen documentos, deberán contar con medidas de seguridad, de acuerdo con lo previsto en el Esquema Nacional de Seguridad, que garanticen la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados. En particular, asegurarán la identificación de los usuarios y el control de accesos, así como el cumplimiento de las garantías previstas en la legislación de protección de datos.»

La Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, contiene similares previsiones en el artículo 3, de Principios Generales, artículo 38, de la sede electrónica, el artículo 46, de archivo electrónico de documentos, el artículo 155, sobre transmisiones de datos entre Administraciones Públicas y el artículo 156.2, sobre el Esquema Nacional de Seguridad.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, tiene por objeto el establecimiento de los principios y requisitos de una política de seguridad en la utilización de medios electrónicos que permita la adecuada protección de la información. El artículo 11 del citado real decreto exige que todos los órganos superiores de las Administraciones Públicas deberán disponer formalmente de su política de seguridad, que se aprobará por el titular del órgano superior correspondiente. Esta política de seguridad se establecerá con base en los principios básicos recogidos en el capítulo II de la propia norma (seguridad integral, gestión de riesgos, prevención, reacción y recuperación, líneas de defensa, reevaluación periódica, y función diferenciada) y desarrollará una serie de requisitos mínimos consignados en el artículo 11.1.

Por otra parte, la protección de las personas físicas en relación con el tratamiento de datos personales, es un derecho fundamental protegido por el artículo 18.4 de la Constitución española. La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, tiene por objeto garantizar estos derechos

de la ciudadanía y adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el 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), y completar sus disposiciones.

Dicha norma, dedica el capítulo tercero del título V, a la figura del Delegado de Protección de Datos, y se refiere al artículo 37.1 del Reglamento que señala que «el responsable y el encargado del tratamiento designarán un delegado de protección de datos siempre que: a) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial».

Por otro lado, el Real Decreto 806/2014, de 19 de septiembre, sobre organización e instrumentos operativos de las tecnologías de la información y las comunicaciones en la Administración General del Estado y sus Organismos Públicos, creó las Comisiones Ministeriales de Administración Digital como órganos colegiados, «encargados de impulsar la transformación digital de la Administración de acuerdo a una Estrategia común en el ámbito de las Tecnologías de la Información y las Comunicaciones».

La Disposición transitoria segunda del citado real decreto, prevé la regulación de las Comisiones Ministeriales de Administración Digital mediante las correspondientes órdenes ministeriales.

En la Disposición adicional cuarta, sobre «Consolidación de las Unidades TIC» del Real Decreto 864/2018, de 13 de julio, por el que se desarrolla la estructura orgánica básica del Ministerio para la Transición Ecológica, se indica que «la División de Tecnologías de la Información del Ministerio de Transición Ecológica promoverá, en colaboración con las Unidades competentes de los organismos públicos adscritos, la consolidación de los recursos humanos, económico-presupuestarios, técnicos y materiales vinculados.»

Por todo ello, mediante esta orden ministerial se procede a la aprobación de la política de seguridad y a la creación de la Comisión Ministerial de Administración Digital, del Ministerio para la Transición Ecológica, y a regular su composición y funciones.

En la elaboración de la orden se han cumplido los principios de buena regulación recogidos en el artículo 129 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y, en particular, los principios de necesidad y eficiencia, pues se trata del instrumento más adecuado para garantizar una política de seguridad en la utilización de medios electrónicos que permita una adecuada protección de la información dentro del Ministerio para la Transición Ecológica, a cuya ejecución coadyuva la creación de la Comisión Ministerial de Administración Digital. También se adecua al principio de proporcionalidad, pues no existe otra alternativa menos restrictiva de derechos o de obligaciones. 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, evitando cargas administrativas innecesarias o accesorias.

En su virtud, con la aprobación previa de la Ministra de Política Territorial y Función Pública, dispongo:

Artículo 1. *Objeto y ámbito de aplicación.*

1. Constituye el objeto de esta orden, la aprobación de la Política de Seguridad de la Información, en adelante PSI, en el ámbito de la Administración Electrónica del Ministerio para la Transición Ecológica, y la creación de la Comisión Ministerial de Administración Digital, en adelante CMAD.

2. La PSI será de obligado cumplimiento para todos los órganos superiores y directivos del Ministerio para la Transición Ecológica, incluidos los organismos públicos vinculados o dependientes del Departamento, que no tengan establecida su propia política de seguridad. En aquellos organismos que tengan su propia política de seguridad, 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 el mismo.

Artículo 2. *Estructura organizativa.*

La estructura organizativa para la gestión de la seguridad de la información, en el ámbito descrito por la PSI del Ministerio para la Transición Ecológica, está compuesta por los siguientes agentes:

1. La CMAD.
2. Los Responsables de la Información.
3. Los Responsables del Servicio.
4. Los Responsables de Seguridad.
5. Los Responsables del Sistema.
6. Los Delegados de Protección de Datos Personales.

Artículo 3. *Principios de la seguridad de la información.*

1. Principios básicos.

Además de los previstos en el artículo 4 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, se establecen los siguientes:

a) Alcance estratégico: La seguridad de la información cuenta con el compromiso y apoyo de todos los niveles directivos, de forma que está coordinada e integrada con el resto de iniciativas estratégicas del Departamento para conformar un todo coherente y eficaz.
b) Proporcionalidad: El establecimiento de medidas de protección, detección y recuperación, deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.
c) Mejora continua: Las medidas de seguridad se reevaluarán y actualizarán periódicamente, para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado, instruido y dedicado.
d) Seguridad por defecto: Los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.

2. Principios particulares y responsabilidades específicas.

Las directrices fundamentales de seguridad se concretan en un conjunto de principios particulares y responsabilidades específicas, que se configuran como objetivos instrumentales, que garantizan el cumplimiento de los principios básicos de la PSI y que inspiran las actuaciones del Departamento en dicha materia. Se establecen los siguientes:

a) Gestión de activos de información: Los activos de información del Departamento se encontrarán inventariados y categorizados, y estarán asociados a un responsable.
b) Seguridad ligada a las personas: Se implantarán los mecanismos necesarios para que cualquier persona que acceda o pueda acceder a los activos de información, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos.
c) Seguridad en la gestión de comunicaciones y operaciones: Se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las tecnologías de la información y comunicaciones. La información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.
d) Control de acceso: Se limitará el acceso a los activos de información por parte de usuarios, procesos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo. Además, quedará registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso y auditar su uso adecuado, conforme a la actividad de la organización.

e) Adquisición, desarrollo y mantenimiento de los sistemas de información: Se contemplarán los aspectos de seguridad de la información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.

f) Gestión de los incidentes de seguridad: Se implantarán los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.

g) Gestión de la continuidad: Se implantarán los mecanismos apropiados, para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de sus procesos de negocio, de acuerdo a las necesidades de nivel de servicio de sus usuarios.

h) 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. 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.

i) Cumplimiento: Se adoptarán las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa en materia de seguridad de la información.

Artículo 4. *Configuración y adscripción de la Comisión Ministerial de Administración Digital.*

La CMAD del Ministerio para la Transición Ecológica, se configura como Comité de Dirección de Seguridad de la Información y como instrumento para la coordinación interna del Departamento en materia de Administración Digital, así como órgano de enlace y colaboración con la Secretaría General de Administración Digital, en adelante SGAD.

La Comisión se adscribe a la Subsecretaría del Departamento y su ámbito de actuación comprenderá a todos los órganos del Ministerio y sus organismos públicos adscritos. La División de Sistemas y Tecnologías de la Información y de las Comunicaciones, dependiente de la Subsecretaría, prestará a la CMAD el apoyo que precise para el desempeño de sus funciones.

Artículo 5. *Composición de la Comisión Ministerial de Administración Digital.*

1. La CMAD tendrá la siguiente composición:

a) Presidencia: La persona titular de la Subsecretaría para la Transición Ecológica.

b) Vicepresidencia: La persona titular de la Subdirección General de Servicios y Coordinación.

c) Vocalías:

El director del Gabinete del Ministro.

El titular del Gabinete de la Secretaría de Estado de Energía.

El titular del Gabinete de la Secretaría de Estado de Medio Ambiente.

Un representante de cada una de las Direcciones Generales del Departamento, designados por sus titulares, con rango mínimo de subdirector general o asimilado.

Un representante de cada uno de los organismos públicos adscritos al Departamento, designados por sus titulares, con rango mínimo de subdirector general o asimilado.

La persona titular de la División de Sistemas y Tecnologías de la Información y de las Comunicaciones, que ejercerá además la Secretaría de la CMAD y actuará con voz y voto.

Cada vocal titular podrá designar como suplente a un funcionario con rango mínimo de Subdirector General o asimilado.

2. El representante de cada uno de los centros directivos, representará y coordinará al resto de unidades dentro del ámbito de su centro directivo, pudiendo asistir a las reuniones, acompañados de funcionarios expertos en las materias a tratar que actuarán como asesores con voz pero sin voto.

3. Se creará un grupo de trabajo, a nivel interno, preparatorio de las reuniones de la CMAD.

Artículo 6. *Funcionamiento de la Comisión Ministerial de Administración Digital.*

1. La CMAD del Ministerio para la Transición Ecológica podrá constituir, convocar, celebrar sesiones, adoptar acuerdos y remitir actas tanto de forma presencial como a distancia.

2. La CMAD se regirá por las normas previstas para los órganos colegiados en la sección 3ª del capítulo II del Título Preliminar de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

3. La CMAD se reunirá, al menos, una vez al año, mediante convocatoria de su Presidente, bien a iniciativa propia, a iniciativa de su Vicepresidente o cuando lo soliciten, al menos, la mitad de sus miembros.

Artículo 7. *Funciones de la Comisión Ministerial de Administración Digital.*

La CMAD desempeñará las siguientes funciones:

a) Ejercer las actuaciones determinadas por la Política de Seguridad de la Información del Departamento (PSI) y específicamente:

1.º Elaborar las propuestas de modificación y actualización permanente que se hagan sobre la PSI.

2.º Aprobar el resto de la normativa de seguridad de primer nivel.

3.º Elaborar estudios, análisis previos y propuestas sobre la normativa de seguridad de segundo y tercer nivel.

4.º Velar e impulsar el cumplimiento de la PSI y de su desarrollo normativo.

5.º Promover la mejora continua en la gestión de la seguridad de la información.

6.º Coordinar la comunicación con el Centro Criptológico Nacional en la utilización de servicios de respuesta a incidentes de seguridad.

7.º Aprobar el Plan de Auditoría y el Plan de Formación propuestos por el Responsable de Seguridad.

8.º Resolver los posibles conflictos que puedan derivarse del establecimiento de la citada estructura organizativa.

b) Ejercerá las funciones incluidas dentro del artículo 7, sobre «Las Comisiones Ministeriales de Administración Digital» del Real Decreto 806/2014, de 19 de septiembre, sobre organización e instrumentos operativos de las tecnologías de la información y las comunicaciones en la Administración General del Estado y sus Organismos Públicos, y específicamente:

1.º Informar los proyectos de disposiciones de carácter general del Departamento sobre su oportunidad, costes y necesidad de recursos humanos y tiempos de desarrollo, que se puedan derivar de la aprobación del proyecto, desde la perspectiva de la utilización de medios y servicios TIC. Este informe será remitido a la SGAD, para su conocimiento y valoración, con periodicidad semestral.

2.º Con la finalidad de conocer todas las propuestas de contratación relacionadas con las TIC, la CMAD será la encargada de canalizar la solicitud de informe preceptivo a la SGAD, conforme a lo establecido en el artículo 16.2 del Real Decreto 806/2014, de 19 de septiembre. Igualmente, y en base a la prestación de servicios mutuos, enviará estas propuestas a la División de Sistemas y Tecnologías de la Información y de las Comunicaciones del Ministerio para la Transición Ecológica.

3.º Coordinar la recogida, agregación e incorporación de la información requerida por la SGAD.

4.º Elaborar, con periodicidad anual, un informe de avance de los Planes de actuación en materia TIC del Departamento y sus organismos públicos para la transformación digital, que recoja el estado de las actuaciones previstas y las contrataciones efectuadas.

La CMAD, para el ejercicio de estas funciones, podrá recabar cuanta información estime precisa de todas las unidades y organismos públicos del Ministerio, que vendrán obligados a facilitarla, de acuerdo con la legislación vigente.

Artículo 8. *Los responsables de la información y los responsables del servicio.*

1. Los responsables de la información y los responsables del servicio tienen la potestad, dentro de su ámbito de actuación y de sus competencias, de establecer los requisitos en materia de seguridad de la información que manejan y de los servicios que prestan. 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. Cada órgano superior o directivo del Ministerio para la Transición Ecológica, así como cada organismo público dependiente del Departamento, a los que conforme al artículo 1 les sea de aplicación esta PSI, designará estos perfiles de acuerdo con su propia organización interna.

Artículo 9. *Los responsables de seguridad.*

1. El responsable de seguridad, es la persona que determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios. Cada órgano superior o directivo del Ministerio para la Transición Ecológica, así como cada organismo público vinculado o dependiente del Departamento a los que sea de aplicación esta PSI, designará un Responsable de Seguridad. En el ámbito de la protección de datos de carácter personal se denomina responsable del tratamiento.

2. El ámbito de actuación de cada responsable de seguridad, se limitará única y exclusivamente, a los sistemas de información y servicios de tecnologías de la información y de las comunicaciones, que sean competencia y responsabilidad directa del centro al que pertenezca dicho responsable de seguridad.

3. Serán funciones de cada responsable de seguridad, dentro del ámbito de actuación enunciado en el punto anterior, 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 y tercer nivel, definida en el artículo 9 y velar e impulsar su cumplimiento por parte de Responsables del Sistema del artículo 8 y de cualquier otro agente del sistema.

c) Encargarse de que la documentación de seguridad se mantenga organizada y actualizada, y de gestionar los mecanismos de acceso a la misma. En el ámbito de la protección de datos se denominará encargado del tratamiento.

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

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

Artículo 10. *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.

2. Cada órgano superior o directivo del Ministerio para la Transición Ecológica contará con la División de Sistemas y Tecnologías de la Información y de las Comunicaciones como responsable del sistema, para aquellos sistemas que se hayan desarrollado con su coordinación. Para el resto de sistemas deberá designar este responsable del desarrollo realizado, operado o mantenido con recursos externos del departamento.

3. Cada organismo público vinculado o dependiente del Departamento a los que, conforme al artículo 1, le sea de aplicación esta PSI, designará este perfil.

Disposición adicional primera. *Instrucciones de ejecución.*

En conformidad con la disposición adicional cuarta del Real Decreto 864/2018, de 13 de julio, por el que se desarrolla la estructura orgánica básica del Ministerio para la Transición Ecológica, sobre Consolidación de las Unidades TIC, la Subsecretaría del Departamento podrá dictar las instrucciones necesarias para la consolidación de recursos TIC y el mejor cumplimiento de esta orden.

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

La aprobación de la PSI, el funcionamiento de la CMAD o la puesta en marcha de medidas de seguridad no supondrá incremento de gasto público, y será atendido con los medios materiales y de personal existentes en el Ministerio para la Transición Ecológica, y con las disponibilidades presupuestarias existentes en cada ejercicio, sin que pueda suponer incremento de dotaciones, ni de retribuciones, ni de otros gastos de personal.

Disposición derogatoria única. *Derogación normativa parcial.*

Se derogan cuantas disposiciones de igual o inferior rango se opongan a lo establecido en esta orden, y en particular en aquellas materias de ámbito competencial del Ministerio para la Transición Ecológica, las siguientes de manera parcial:

1. La Orden AAA/1231/2015, de 17 de junio, por la que se crea la Comisión Ministerial de Administración Digital del Ministerio de Agricultura, Alimentación y Medio Ambiente (CMAD) y se regula su composición y funciones y la Orden AAA/991/2015, de 21 de mayo, por la que se aprueba la política de seguridad de la información en el ámbito de la Administración Electrónica del Ministerio de Agricultura, Alimentación y Medio Ambiente, quedan sin efecto en relación a la participación en sus órganos y obligaciones de unidades dependientes del Ministerio para la Transición Ecológica.

2. Igualmente 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 y la Orden ETU/433/2018, de 17 de abril, por la que se crea la Comisión Ministerial de Administración Digital en el Ministerio de Energía, Turismo y Agenda Digital, y se regula su composición y funcionamiento, quedan sin efecto en relación a la participación en sus órganos y obligaciones de unidades dependientes del Ministerio para la Transición Ecológica.

Disposición final única. *Entrada en vigor.*

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

Madrid, 15 de abril de 2019.–La Ministra para la Transición Ecológica, Teresa Ribera Rodríguez.