I. DISPOSICIONES GENERALES

MINISTERIO DE UNIVERSIDADES

18486 *Orden UNI/1231/2021, de 5 de noviembre, por la que se aprueba la política de seguridad de la información en el ámbito de la administración electrónica y de protección de datos y se crea la Comisión Ministerial de Administración Digital del Ministerio de Universidades.*

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 otra parte, 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 (ENS), 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 establece que las Administraciones Públicas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos. Dichos medios deben asegurar la interoperabilidad y seguridad de los sistemas y soluciones adoptadas, garantizarán la protección de los datos de carácter personal y facilitarán preferentemente la prestación conjunta de servicios a los interesados. En este sentido, destacan las previsiones contenidas en el artículo 3, de principios generales, el 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 sobre el Esquema Nacional de Seguridad y el Esquema Nacional de Interoperabilidad.

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 estableció los principios y requisitos de una política de seguridad en la utilización de medios electrónicos que permita la adecuada protección de la información. En concreto, en su artículo 11 exige que todos los órganos superiores de las Administraciones Públicas dispongan formalmente de su política de seguridad, que se aprobará por el titular del órgano superior correspondiente, se establecerá con base en los principios básicos recogidos en su capítulo II (seguridad integral, gestión de riesgos, prevención, reacción y recuperación, líneas de defensa, reevaluación periódica, y función diferenciada) y desarrollará una serie de requisitos mínimos previstos en su artículo 11.1.

El Reglamento de actuación y funcionamiento del sector público por medios electrónicos, aprobado por el Real Decreto 203/2021, de 30 de marzo, desarrolla la Ley 39/2015, de 1 de octubre, y la Ley 40/2015, de 1 de octubre, en lo referente a la actuación y funcionamiento electrónico del sector público. Establece como principio general el principio de proporcionalidad, en cuya virtud sólo se exigirán las garantías y medidas de seguridad adecuadas a la naturaleza y circunstancias de los distintos trámites y actuaciones electrónicos. En relación con la ciberseguridad y la seguridad de las redes y sistemas de información, establece tanto los sistemas de identificación, firma y verificación de las Administraciones Públicas como los de los interesados en los procedimientos, así como las características y forma de aprobación y de autorización de los sistemas de clave concertada o cualquier otro sistema que las Administraciones

cve: BOE-A-2021-18486
Verificable en https://www.boe.es

Públicas consideren válido para la identificación electrónica de las personas. El nivel de seguridad en la identificación electrónica exigido en los procedimientos y servicios se deberá definir y publicar en la sede electrónica, de acuerdo con el Reglamento (UE) n.º 910/2014, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE. Este nivel de seguridad en la identificación electrónica del sistema de información que soporta el procedimiento o servicio se determinará sobre la base del análisis de riesgos, de acuerdo con el Esquema Nacional de Seguridad y la normativa correspondiente. La disposición adicional primera del Real Decreto 4/2010, de 8 de enero modificado por el Real Decreto 203/2021, establece el desarrollo del Esquema Nacional de Interoperabilidad, a través de una serie de normas técnicas de interoperabilidad que serán de obligado cumplimiento por parte de las Administraciones Públicas. La disposición adicional tercera del reglamento citado crea el nodo de interoperabilidad de identificación electrónica del Reino de España para el reconocimiento mutuo de identidades electrónicas entre los Estados miembros, de acuerdo con lo previsto en el Reglamento (UE) n.º 910/2014, de 23 de julio de 2014.

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. El artículo 24 del 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) establece como obligaciones generales del responsable y del encargado del tratamiento la aplicación de las medidas técnicas y organizativas apropiadas, entre las que se encuentran las oportunas políticas de protección de datos, que cumplan en particular los principios de protección de datos desde el diseño y por defecto.

Asimismo, el artículo 32 del Reglamento general de protección de datos atribuye al responsable y encargado del tratamiento responsabilidades en materia de seguridad de los datos personales, si bien con un enfoque distinto al aplicado para la seguridad de la información porque los activos a proteger son los derechos y libertades de las personas.

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, 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 su parte, las guías publicadas por el Centro Criptológico Nacional, CCN-STIC 801, sobre responsabilidades y funciones en el ENS, y la CCN-STIC 881, Impacto del Reglamento General de Protección de Datos en el ENS, orientan hacia un planteamiento conjunto de la protección de datos y la seguridad de la información.

Adicionalmente, la Ley 10/2021, de 9 de julio, de trabajo a distancia, regula los derechos de los trabajadores en relación con el uso de medios tecnológicos y digitales. En su artículo 20 determina que, las personas trabajadoras, en el desarrollo del trabajo a distancia, deberán cumplir las instrucciones que haya establecido la empresa en el marco de la legislación sobre protección de datos y sobre seguridad de la información específicamente fijadas por la empresa.

Particularmente en la actualidad, cuando el teletrabajo y las relaciones de carácter remoto con los ciudadanos se han intensificado en la actividad administrativa, es tan indispensable como urgente dar a conocer a la ciudadanía en general y a los empleados públicos en particular el contenido de las políticas de seguridad y de privacidad que se vienen aplicando, en el ámbito de la administración electrónica, en el Ministerio de Universidades.

Por otra parte, 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

cve: BOE-A-2021-18486
Verificable en https://www.boe.es

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 con una Estrategia común en el ámbito de las Tecnologías de la Información y las Comunicaciones».

La disposición transitoria segunda del citado Real Decreto 806/2014, de 19 de septiembre, prevé la regulación de las Comisiones Ministeriales de Administración Digital mediante las correspondientes órdenes ministeriales.

Por su parte, en la disposición adicional cuarta, sobre «Actuaciones en materia de tecnologías de la información y las comunicaciones», del Real Decreto 431/2020, de 3 de marzo, por el que se desarrolla la estructura orgánica básica del Ministerio de Universidades, se indica que se promoverá la consolidación de los recursos humanos, económico-presupuestarios, técnicos y materiales vinculados en materia de tecnologías de la información y las comunicaciones. Por ello, se propone un órgano que coordine las unidades de tecnologías de la información y las comunicaciones de los organismos autónomos, dentro del Ministerio.

El Ministerio de Universidades ha optado por adoptar una política conjunta de seguridad de la información y protección de datos que permita recoger y delimitar con claridad las responsabilidades y funciones en los dos ámbitos, de forma que se aborden tanto las cuestiones comunes como aquellas que resultan propias de cada uno de ellos.

Por todo lo anterior, mediante esta orden ministerial se procede a la aprobación de la política de seguridad y de protección de datos del departamento y a la creación de la Comisión Ministerial de Administración Digital del Ministerio de Universidades 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 y de protección de datos que permita una adecuada protección de la información dentro del Ministerio, 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 y transparencia, 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 Hacienda y Función Pública, dispongo:

Artículo 1. *Objeto y ámbito de aplicación.*

1. El objeto de esta orden es establecer la política de protección de datos y de seguridad de la información (en adelante PPDSI) y la creación de la Comisión Ministerial de Administración Digital (en adelante CMAD) del Ministerio de Universidades.

2. La PPDSI se aplicará a todos los sistemas de información y a todas las actividades de tratamiento de datos de carácter personal de los que sea responsable el Ministerio de Universidades.

3. La PPDSI será de obligado cumplimiento para todos los órganos superiores y directivos del Ministerio, 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.

4. La PPDSI será de obligado cumplimiento para todo el personal que acceda, tanto a los sistemas de información, como a la propia información de la que es responsable el departamento y sus organismos públicos adscritos, con independencia de cuál sea su destino, adscripción o relación con el mismo.

cve: BOE-A-2021-18486
Verificable en https://www.boe.es

Artículo 2. *Principios de protección de datos y 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, el Ministerio de Universidades tratará la información y los datos personales bajo su responsabilidad conforme a los principios de protección de datos y seguridad de la información establecidos en el artículo 5 del 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).

Asimismo, se establece lo siguiente:

a) Atención de los derechos de las personas afectadas: se adoptarán medidas en la organización que garanticen el adecuado ejercicio por las personas afectadas, cuando proceda, de los derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento y portabilidad respecto de sus datos de carácter personal.

b) Alcance estratégico: la protección de datos y la seguridad de la información debe contar con el compromiso y apoyo de todos los niveles directivos, de forma que se coordine e integre con el resto de las iniciativas estratégicas del departamento para conformar un todo coherente y eficaz.

c) Responsabilidad diferenciada: en los sistemas de información del Ministerio de Universidades se observará el principio de responsabilidad diferenciada. Las responsabilidades y funciones se delimitarán de la siguiente manera, sin perjuicio de lo establecido en la normativa en materia de protección de datos:

1.º Responsable del tratamiento: determina los fines y medios del tratamiento.

2.º Encargado del tratamiento: trata datos personales por cuenta del responsable del tratamiento según sus requerimientos.

3.º Persona designada como delegado de protección de datos: informa y asesora al responsable del tratamiento de las obligaciones en materia de cumplimiento del Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016.

4.º Responsable de la información: determina los requisitos de seguridad de la información tratada.

5.º Responsable del servicio: determina los requisitos funcionales y de seguridad de los servicios prestados a partir de la información.

6.º Responsable del sistema: tiene la responsabilidad sobre los requisitos no funcionales y de diseño, construcción, operación y soporte de los sistemas de información utilizados en la prestación de los servicios.

7.º Responsable de seguridad de la información: determina las decisiones para satisfacer los requisitos de seguridad.

d) Gestión de riesgos: Al evaluar el riesgo, se tendrán en cuenta los riesgos que se derivan para los derechos de las personas con respecto al tratamiento de sus datos personales.

e) Proporcionalidad: Se establecerán medidas de protección, detección y recuperación que resulten proporcionales a los potenciales riesgos y a la criticidad y valor de la información, de los tratamientos de datos personales y de los servicios afectados.

f) Proceso de verificación: Se implantará un proceso de verificación, evaluación y valoración regulares, de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad de los tratamientos.

g) Protección de datos y seguridad desde el diseño y por defecto: se adoptarán las medidas técnicas y organizativas que corresponda implantar para atender los riesgos

cve: BOE-A-2021-18486
Verificable en https://www.boe.es

generados por el tratamiento de acuerdo con lo exigido por el citato Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

h) 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.

2. Principios particulares y responsabilidades específicas.

Los principios particulares y responsabilidades específicas garantizan el cumplimiento de los principios básicos de la PPDSI e inspiran las actuaciones del departamento en materia de protección de datos y seguridad de la información. Se establecen, como mínimo, los siguientes:

a) Registro de las actividades de tratamiento y gestión de activos de información. Se mantendrá un registro de las actividades de tratamiento, en los términos previstos en el artículo 4, cuyo inventario se hará público en la sede electrónica del Ministerio de Universidades. Asimismo, los activos de información se encontrarán inventariados y categorizados y estarán asociados a una unidad responsable.

b) Seguridad ligada a las personas. Se implementarán los mecanismos necesarios para que cualquier persona que acceda o pueda acceder a los activos de información y a los datos de carácter personal, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos. El nivel de seguridad en la identificación electrónica exigido en los procedimientos y servicios se definirá y publicará en la sede electrónica.

c) Seguridad física. Los activos de información serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.

d) 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. El sistema ha de proteger el perímetro, en particular si se conecta a redes públicas. En todo caso, se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas y se controlará su punto de unión.

e) Control de acceso. Se limitará el acceso a los activos de información por parte de las personas usuarias, 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. Para corregir, o exigir responsabilidades en su caso, cada persona que acceda a la información del sistema debe estar identificada de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos y quién ha realizado determinada actividad. En caso de existir indicios de actividades delictivas o que comprometan la seguridad de la información tratada por el Ministerio de Universidades, éstos deberán ser comunicados a la autoridad competente para su persecución.

f) 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.

g) Gestión de los incidentes de seguridad. Se establecerán los mecanismos apropiados para la correcta identificación, registro, resolución y notificación, en los

cve: BOE-A-2021-18486
Verificable en https://www.boe.es

términos previstos en la normativa de protección de datos y seguridad de la información de los incidentes de seguridad.

h) Gestión de la continuidad. Se implementarán los mecanismos apropiados, para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de sus procesos de negocio, de acuerdo con las necesidades de nivel de servicio de sus usuarios.

i) Gestión de riesgos. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables, de acuerdo con el artículo 6 del Real Decreto 3/2010, de 8 de enero. Se realizará un análisis de riesgos de manera continua sobre los sistemas de información que incluirá 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.

j) Cumplimiento. Se adoptarán las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa en materia de seguridad de la información y protección de datos de carácter personal.

k) Profesionalidad. La seguridad de los sistemas estará atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida (instalación, mantenimiento, gestión de incidencias y desmantelamiento). El personal del Ministerio de Universidades recibirá la formación específica necesaria para que conozca la PPSSI del Departamento y la normativa aplicable en la materia, para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios de la Administración. El Ministerio de Universidades exigirá que las organizaciones que le presten servicios de seguridad cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados.

l) Uso aceptable de los sistemas de información: en el caso del personal al servicio del Ministerio de Universidades, los medios y equipos informáticos a utilizar serán directamente provistos e instalados por las unidades de administración de sistemas informáticos y comunicaciones o por los proveedores de servicios, como parte del acuerdo de prestación que se establezca, con conocimiento y autorización de las unidades técnicas encargadas a tal efecto, siendo el único uso aceptable de los mismos el adecuado desempeño de las funciones propias de su puesto de trabajo y quedando prohibida toda alteración no autorizada de los mismos.

Artículo 3. *Estructura organizativa.*

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

a) La CMAD.
b) Las personas responsables de la información.
c) Las personas responsables del servicio.
d) Las personas responsables de la seguridad de la información.
e) Las personas responsables del sistema.
f) Las personas responsables del tratamiento.
g) La persona designada como delegado de protección de datos.

Artículo 4. *Registro de actividades de tratamiento.*

El Ministerio de Universidades mantendrá actualizado el registro de las actividades de tratamiento con datos de carácter personal de las que sea responsable, que incluirá toda la información a la que se refiere el artículo 30 del Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016 y el artículo 31 de la Ley

cve: BOE-A-2021-18486
Verificable en https://www.boe.es

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

El registro de actividades de tratamiento podrá consultarse en el portal del Ministerio de Universidades.

Artículo 5. *Creación y adscripción de la Comisión Ministerial de Administración Digital.*

La CMAD del Ministerio de Universidades se configura como un órgano colegiado de ámbito departamental responsable del impulso y de la coordinación interna en materia de Administración Digital. La CMAD estudiará y planificará las necesidades funcionales de las distintas unidades del ministerio, valorará las posibles vías de actuación, priorizándolas, y propondrá su desarrollo, todo ello evitando que se generen duplicidades, conforme al principio de racionalización, y promoviendo la compartición de infraestructuras y la utilización de medios y servicios digitales comunes y transversales.

Asimismo, ejercerá sus funciones como comité de dirección de seguridad de la información, así como órgano de enlace y colaboración con la Secretaría General de Administración Digital, en adelante SGAD.

La CMAD 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 6. *Composición de la Comisión Ministerial de Administración Digital.*

1. La CMAD del Ministerio de Universidades actúa en Pleno y Comisión Permanente.

2. El Pleno de la CMAD tendrá la siguiente composición:

a) Presidente: la persona titular de la Subsecretaría de Universidades.
b) Vicepresidente: la persona titular del Gabinete Técnico de la Subsecretaría.
c) Vocales, en representación de los siguientes órganos:

1.º La persona titular del Gabinete del Ministro.
2.º Secretaría General de Universidades.
3.º Secretaría General Técnica.
4.º Cada organismo público adscrito al Departamento.
5.º La persona titular de la División de Tecnologías de la Información y la Comunicación.
6.º La persona titular de la Abogacía del Estado en el Departamento.
7.º La persona titular de la Subdirección General de Gestión Económica, Oficina Presupuestaria y Asuntos Generales.
8.º La persona designada como delegado de protección de datos del Departamento.

En los supuestos 2.º, 3.º y 4.º las vocalías serán designadas por la persona titular del órgano representado entre quienes ostenten rango mínimo de Subdirector General.

d) Secretario: un funcionario de la División de Tecnologías de la Información y la Comunicación, como mínimo con nivel 26, que actuará con voz y sin voto, designado por el titular de la División.

3. En caso de vacante, ausencia, enfermedad, u otra causa legal de la persona que ejerza la Presidencia, y en general cuando concurra alguna causa justificada, ésta será sustituida por la persona que ocupe la Vicepresidencia. En ausencia de esta última, la Presidencia será asumida por la vocalía de mayor jerarquía, antigüedad y edad, por este orden.

cve: BOE-A-2021-18486
Verificable en https://www.boe.es

En casos de vacante, ausencia, enfermedad, u otra causa legal de las vocalías titulares, y en general cuando concurra alguna causa justificada, las mismas serán sustituidas por sus suplentes. Las vocalías suplentes serán designadas, en cada caso, por el titular de la vocalía.

La persona que ocupa la Secretaría será sustituida en casos de vacante, ausencia, enfermedad, u otra causa legal y en general cuando concurra alguna causa justificada por un funcionario, con nivel 26 o superior de la Subdirección General de Tecnologías de la Información y Comunicaciones, designado por el titular de dicha Subdirección General.

4. La Comisión Permanente de la CMAD tendrá la siguiente composición:

a) Presidente: la persona titular de la División de Tecnologías de la Información y la Comunicación.

b) Vicepresidente: un funcionario de la División de Tecnologías, como mínimo de nivel 28, designado por el titular de la División.

c) Vocales, en representación de los siguientes órganos:

1.º La Secretaría General de Universidades.

2.º Cada organismo público adscrito al Departamento, designados por sus titulares, cuando se refieran a ese organismo los temas a tratar en la reunión.

3.º La Subdirección General de Gestión Económica, Oficina Presupuestaria y Asuntos Generales.

4.º La persona designada como delegado de protección de datos en el ámbito del Ministerio

Los vocales tendrán un nivel 28 o superior, serán designados por la persona titular del centro directivo al que representen que podrán designar como suplente a un funcionario con rango mínimo de nivel 26 o superior.

d) Secretario: un funcionario de la División de Tecnologías de la Información y la Comunicación, como mínimo con nivel 26, que actuará con voz y sin voto, designado por el titular de la División.

5. La persona representante de cada uno de los centros directivos coordinará a todas las unidades dentro del ámbito de su centro directivo, pudiendo asistir a las reuniones acompañada de funcionario experto en las materias a tratar que actuarán como asesores con voz, pero sin voto.

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

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

2. La CMAD del Ministerio de Universidades podrá constituirse, convocar y celebrar sesiones, adoptar acuerdos y remitir actas tanto de forma presencial como a distancia.

3. El Pleno de 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.

4. La Comisión Permanente se reunirá con periodicidad mensual, si bien la Presidencia de esta podrá convocarla con carácter extraordinario cuando resulte necesario.

Artículo 8. *Funciones de la Comisión Ministerial de Administración Digital.*

1. La CMAD ejercerá las funciones recogidas en el artículo 7 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.

cve: BOE-A-2021-18486
Verificable en https://www.boe.es

2. El Pleno desempeñará las siguientes funciones:

a) Actuar como órgano de relación entre el Ministerio de Universidades y sus organismos adscritos y la SGAD, para asegurar la coordinación con los criterios y políticas definidas por ésta.

b) Impulsar, ejecutar y supervisar, en el ámbito del Departamento, el cumplimiento de las directrices y el seguimiento de las pautas de actuación recogidas en la Estrategia TIC de la Administración General del Estado y sus organismos públicos aprobada por el Gobierno a propuesta de la Comisión de Estrategia TIC.

c) Promover la transformación digital, en el marco de las directrices establecidas por la SGAD.

d) Impulsar la digitalización de los servicios y procedimientos del Departamento con el fin de homogeneizarlos, simplificarlos, mejorar su calidad y facilidad de uso, así como las prestaciones ofrecidas a los ciudadanos y empresas, optimizando la utilización de los recursos TIC disponibles.

e) Elaborar, y evaluar periódicamente, el Plan de acción del Departamento para la transformación digital, desarrollando los criterios establecidos por la Secretaria General de Administración Digital, atendiendo a la Estrategia TIC de la Administración General del Estado y sus organismos públicos, aprobada por el Consejo de Ministros.

f) Aprobar las propuestas de modificación y actualización que se hagan sobre la PPDSI.

g) Aprobar el Plan de auditoría y el Plan de formación propuestos por el Responsable de Seguridad.

3. La Comisión Permanente desempeñará las siguientes funciones:

a) Apoyar al Pleno en la elaboración del Plan de acción del Departamento para la transformación digital, previsto en el artículo 7.3.c) del Real Decreto 806/2014, de 19 de septiembre.

b) Analizar las necesidades funcionales de las unidades de gestión del departamento y sus organismos adscritos y evaluar las distintas alternativas de solución propuestas por la unidad TIC, identificando las oportunidades de mejora de eficiencia que pueden aportar las TIC, aplicando soluciones ya desarrolladas en el ámbito del Sector Público y estimando costes en recursos humanos y materiales que los desarrollos TIC asociados puedan suponer.

c) Informar, desde la perspectiva de la utilización de medios y servicios TIC, los proyectos de disposiciones de carácter general del departamento y específicamente sobre su oportunidad, aplicación, costes económicos, necesidad de recursos humanos tanto para su desarrollo como para su mantenimiento y operación y tiempos de desarrollo e implantación, que se deriven de la aprobación del proyecto.

d) 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, enviará estas propuestas a la División de Tecnologías de la Información y la Comunicación del Ministerio de Universidades.

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

f) Elaborar, con periodicidad anual, un informe de avance de los planes de actuación en materia tecnologías de información y comunicación del departamento y sus organismos públicos para la transformación digital, que recoja el estado de las actuaciones previstas y las contrataciones efectuadas.

g) Ejercer las actuaciones determinadas por la PPDSI del departamento y específicamente:

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

cve: BOE-A-2021-18486
Verificable en https://www.boe.es

2.º Velar e impulsar el cumplimiento de la PPDSI y de su desarrollo normativo.
3.º Promover la mejora continua en la gestión de la seguridad de la información.
4.º Coordinar la comunicación con el Centro Criptológico Nacional en la utilización de servicios de respuesta a incidentes de seguridad.

La CMAD, para el ejercicio de estas funciones, podrá recabar cuanta información estime precisa de todas las unidades y organismos públicos del Ministerio.

Artículo 9. *Las personas responsables del tratamiento.*

1. Les corresponde determinar los fines y medios del tratamiento y aplicar las medidas técnicas y organizativas apropiadas a fin de garantizar un nivel de seguridad adecuado al riesgo para los derechos y libertades de las personas, a propuesta de la CMAD o, en su caso, del responsable o responsables de seguridad de la información, teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, conforme a lo exigido en el Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, la Ley Orgánica 3/2018, de 5 de diciembre y el Real Decreto 3/2010, de 8 de enero.
2. Asimismo, es el responsable de la transmisión de las obligaciones al encargado del tratamiento y la verificación del cumplimiento de estas.
3. Cada órgano superior o directivo del Ministerio de Universidades, así como cada organismo público dependiente del departamento, a los que conforme al artículo 1 les sea de aplicación esta PPDSI, designará a las personas responsables del tratamiento de acuerdo con su propia organización interna.

Artículo 10. *La persona designada como delegado de protección de datos.*

La Vicesecretaría General Técnica ejercerá las funciones atribuidas a la Secretaría General Técnica en relación con sus competencias relativas al delegado de protección de datos, previstas en el artículo 39 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, para el ámbito del Ministerio, excluyendo sus organismos públicos, que podrán nombrar otras delegaciones o delegados de protección de datos cuando sus necesidades específicas así lo requieran.
En el desempeño de sus tareas, la persona designada como delegado de protección de datos tendrá acceso a los datos personales y procesos de tratamiento.

Artículo 11. *Las personas responsables de la información y responsables del servicio.*

1. Las personas responsables de la información y las personas responsables de servicio podrán establecer, dentro de su ámbito de actuación y de sus competencias, 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. Las funciones del responsable de la información serán la aprobación formal de los niveles y medidas de seguridad de la información y las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo para los derechos y libertades de las personas, teniendo en cuenta el estado de la técnica, el coste de su aplicación y la naturaleza, el alcance, el contexto y los fines del tratamiento.
3. Las funciones del responsable del servicio serán las de establecer los requisitos del servicio y los niveles de seguridad de este para los procedimientos administrativos de su competencia, en cuyo ámbito se lleve a cabo el tratamiento de datos de carácter personal.
4. Cada órgano superior o directivo del Ministerio de Universidades, así como cada organismo público dependiente del departamento, a los que conforme al artículo 1 les sea de aplicación esta PPDSI, designará estos perfiles de acuerdo con su propia organización interna.

cve: BOE-A-2021-18486
Verificable en https://www.boe.es

Artículo 12. *Las personas responsables del sistema.*

1. La persona responsable del sistema desarrollará, operará y mantendrá el sistema de información durante todo su ciclo de vida.

2. La División de Tecnologías de la Información y la Comunicación del Ministerio de Universidades actuará como responsable del sistema para todos aquellos sistemas que se hayan desarrollado o implantado bajo su coordinación. Para el resto de los sistemas, cada órgano superior o directivo deberá designar una persona responsable del desarrollo realizado, operado o mantenido con otros recursos.

3. Cada organismo público vinculado o dependiente del departamento a los que, conforme al artículo 1, le sea de aplicación esta PPDSI, designará a las personas responsables del sistema.

Artículo 13. *Las personas responsables de seguridad de la información.*

1. La persona responsable de seguridad determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios y la seguridad en el tratamiento de los datos personales. El Ministerio de Universidades o cada órgano superior o directivo si se estima conveniente, así como cada organismo público vinculado o dependiente del departamento a los que sea de aplicación esta PPDSI, designará una persona responsable de seguridad, que actuará también como responsable del tratamiento en el ámbito de la protección de datos de carácter personal.

El responsable de seguridad será designado por el titular del Departamento o centro directivo correspondiente. Si en la unidad existe algún servicio con competencias en materia de protección de datos personales y seguridad de la información, su titular ostentará la condición de responsable de seguridad de la información.

Los responsables de seguridad contarán con el apoyo técnico, jurídico y organizativo, tanto de su unidad como del Departamento.

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. Las funciones de cada responsable de seguridad, dentro del ámbito de actuación enunciado en el punto anterior, serán 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 14, y velar e impulsar su cumplimiento por parte de los responsables del tratamiento, de la información, del servicio y 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.

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.

f) Dirigir y coordinar la respuesta a los incidentes de seguridad.

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

h) Elaborar el Plan de auditoría y el Plan de formación.

cve: BOE-A-2021-18486
Verificable en https://www.boe.es

Artículo 14. *Estructura documental y normativa.*

1. El cuerpo documental sobre seguridad de la información se desarrollará en cuatro niveles por ámbito de aplicación, nivel de detalle técnico y de obligado cumplimiento, de manera que cada documento de un determinado nivel de desarrollo se fundamente en los documentos de nivel superior. Dichos niveles de desarrollo documental son los siguientes:

a) Primer nivel. Política de seguridad de la información.

Está constituido por la presente orden y es de obligado cumplimiento, al amparo de lo establecido por el Real Decreto 3/2010, de 8 de enero.

b) Segundo nivel. Directrices y recomendaciones de seguridad.

El cuerpo documental, que comprende las directrices y recomendaciones de seguridad de las tecnologías de la información y las comunicaciones (STIC) y las guías STIC, es de obligado cumplimiento, según lo establecido por el Real Decreto 3/2010, de 8 de enero, y se formalizará mediante aprobación de la CMAD. Las recomendaciones consistirán en buenas prácticas y consejos no vinculantes para mejorar las condiciones de seguridad.

c) Tercer nivel. Procedimientos e instrucciones técnicas.

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

d) Cuarto nivel. Informes, registros y evidencias electrónicas.

Está constituido por los informes técnicos, que son documentos de carácter técnico que recogen el resultado y las conclusiones de un estudio o de una evaluación; registros de actividad o alertas de seguridad, que son documentos de carácter técnico que recogen amenazas y vulnerabilidades a sistemas de información.

2. El comité de dirección de seguridad de la información establecerá los mecanismos necesarios para compartir la documentación derivada del desarrollo documental con el propósito de normalizarlo, en la medida de lo posible, en todo el ámbito de aplicación de la política.

Artículo 15. *Análisis de riesgos, evaluación de impacto en la protección de datos y gestión de los riesgos de seguridad de la información.*

1. Cuando la información contenga datos personales se llevará a cabo, de forma periódica y al menos cada dos años, y, en cualquier caso, con carácter previo a un nuevo tratamiento y siempre que exista un cambio significativo en los sistemas de información y/o en los tratamientos de datos personales, un análisis de riesgos que permita identificar y gestionar los riesgos minimizándolos hasta los niveles que puedan considerarse aceptables.

2. La gestión de riesgos de seguridad de la información debe realizarse de manera continua sobre el sistema de información, conforme a los principios de gestión de la seguridad basada en los riesgos y en la reevaluación periódica.

cve: BOE-A-2021-18486
Verificable en https://www.boe.es

El responsable de seguridad de la información es la persona encargada de recomendar un marco de directrices básicas para armonizar los criterios a seguir para la valoración de riesgos.

El responsable de la Información y el responsable del servicio son los encargados de la gestión de los riesgos sobre la información y sobre los servicios, respectivamente, siendo responsables de su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.

Artículo 16. *Notificación de violaciones de seguridad de los datos personales e incidentes de seguridad de la información.*

El Ministerio de Universidades adoptará las medidas necesarias para garantizar la notificación de las violaciones de seguridad de los datos personales que pudieran producirse a través del procedimiento de notificación de brechas de seguridad establecido al efecto, de conformidad con lo dispuesto en el artículo 33 del Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016.

Igualmente adoptará las medidas procedentes para la comunicación a los interesados que pudieran haberse visto afectados por la violación de seguridad de los datos de carácter personal, en los casos y conforme a lo dispuesto en el artículo 34 del Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016.

Artículo 17. *Resolución de conflictos.*

En caso de conflicto entre los diferentes responsables que componen la estructura organizativa de la política de protección de datos y seguridad de la información, corresponderá la resolución de este a la CMAD, asistido por el responsable de la información.

Artículo 18. *Obligaciones del personal.*

El personal al servicio del Ministerio de Universidades, y de los organismos públicos dependientes del departamento a los que les sea de aplicación esta PPDSI conforme al artículo 1, prestará su colaboración en las actuaciones de implementación de la política de protección de datos y seguridad de la información.

Dicho personal tiene la obligación de conocer y cumplir lo previsto en la PPDSI, así como los instrumentos y procedimientos que la desarrollen.

El personal al servicio del Ministerio de Universidades tiene asimismo el deber de colaborar en la mejora de los principios y requisitos en materia de protección de datos y seguridad de la información evitando o, en su caso, aminorando los riesgos a los que se encuentra expuesta la información y los datos personales de los que es responsable el Ministerio de Universidades. A tal efecto, comunicará a los integrantes de la estructura organizativa de la política de protección de datos y seguridad de la información cualquier propuesta o sugerencia que ayude a preservar la confidencialidad, la integridad y la disponibilidad de la información.

Artículo 19. *Concienciación y formación.*

Se desarrollarán actividades formativas específicas orientadas a la concienciación y formación del personal que presta sus servicios en el Ministerio de Universidades, así como a la difusión de la PPDSI establecida en la presente orden y de los instrumentos de desarrollo.

El Ministerio de Universidades dispondrá de los medios necesarios para que todas las personas con acceso a la información sean informadas acerca de sus deberes y obligaciones, así como de los riesgos existentes en el tratamiento de la información.

cve: BOE-A-2021-18486
Verificable en https://www.boe.es

La persona delegada de protección de datos supervisará las acciones de concienciación y formación del personal que participa en las operaciones de tratamiento con datos personales, a fin de garantizar el cumplimiento de la PPDSI.

Disposición adicional primera. *Instrucciones de ejecución.*

En conformidad con la disposición adicional cuarta del Real Decreto 431/2020, de 3 de marzo, por el que se desarrolla la estructura orgánica básica del Ministerio de Universidades, sobre actuaciones en materia de tecnologías de la información y las comunicaciones, la Subsecretaría del departamento podrá dictar las instrucciones necesarias para la consolidación de recursos humanos, económico-presupuestarios, técnicos y materiales vinculados a dichas tecnologías de la información y la comunicación y para el mejor cumplimiento de esta orden.

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

La aprobación de la PPDSI, la puesta en marcha de medidas de seguridad o el funcionamiento de la CMAD no supondrán incremento de gasto público y serán atendidos con los medios materiales y de personal existentes en el departamento, 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.*

Se derogan cuantas disposiciones de igual o inferior rango se opongan a lo establecido en esta orden, y, en particular, queda derogada exclusivamente respecto al ámbito de competencias del Ministerio de Universidades, la Orden CNU/597/2019, de 30 de mayo, por la que se crea y regula el funcionamiento de la Comisión Ministerial de Administración Digital del Ministerio de Ciencia, Innovación y Universidades.

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, 5 de noviembre de 2021.–El Ministro de Universidades, Manuel Castells Oliván.

cve: BOE-A-2021-18486
Verificable en https://www.boe.es