Resolución de 2 de julio de 2019 de la Directora de la Agencia Española de Protección de Datos, Autoridad Administrativa Independiente (AEPD), por la que se aprueba la Política de protección de datos y seguridad de la información de la AEPD y se derogan las resoluciones de la Directora de la Agencia de 10 de mayo de 2018, por la que se aprueba la Política de protección de datos y seguridad de la información de la Agencia Española de Protección de datos, y la resolución de 15 de junio de 2016, por la que se aprueba la política de seguridad de la información de la AEPD.

Mediante resolución de 10 de mayo de 2018 de la Directora de la Agencia Española de Protección de Datos se aprobó la Política de protección de datos y seguridad de la información de la Agencia Española de Protección de Datos. La publicación de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) hace necesario realizar algunas modificaciones en la citada Política fundamentalmente en lo referente al marco normativo aplicable, que queda redactada de la forma en la que a continuación se señala. La AEPD entiende que, para una mayor seguridad jurídica, y comprensión por los interesados, la presente resolución no ha de limitarse a modificar parcialmente la Política de protección de datos y seguridad de la información, sino que la misma ha de quedar integrada en un documento íntegro, comprensivo de la totalidad de dichas políticas, para que no haya que consultar estas en textos dispersos o separados, sino en un único texto.

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, RGPD), de plena aplicación a partir del 25 de mayo de 2018 conforme a su artículo 99.2, señala que la protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos de dicho Reglamento. A fin de poder demostrar la conformidad con el Reglamento, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto.

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

Por su parte, la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, recoge en su artículo 13, sobre derechos de las personas en sus relaciones con las Administraciones Públicas, el relativo a la protección de datos de carácter personal y, en

particular, a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.

La Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece que las Administraciones Públicas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos. Dichos medios deben asegurar la interoperabilidad y seguridad de los sistemas y soluciones adoptadas, garantizarán la protección de los datos de carácter personal y facilitarán preferentemente la prestación conjunta de servicios a los interesados. En este sentido, el artículo 156 de la citada Ley 40/2015, de 1 de octubre, regula el Esquema Nacional de Seguridad.

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, modificado parcialmente por el Real Decreto 951/2015, de 23 de octubre, establece los principios básicos y los requisitos mínimos que permitan una protección adecuada de la información y tiene por objeto determinar la política de seguridad en la utilización de medios electrónicos en su ámbito de aplicación.

El artículo 11 del citado Real Decreto 3/2010, de 8 de enero, 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. 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 ya mencionado artículo 11.1.

En cumplimiento de dichas disposiciones, la AEPD adoptó mediante resolución de la Directora de la Agencia de 15 de junio de 2016 su política de seguridad de la información en el ámbito de la administración electrónica y el tratamiento de datos personales de la Agencia Española de Protección de Datos, aplicable a todos los sistemas de información, a todas las unidades que conforman la estructura de la Agencia y a todo el personal con acceso a la información de la que es titular la Agencia con independencia de su destino, condición laboral o relación por la que se accede a la información.

La política de protección de datos y de la seguridad de la información es el documento base mediante el cual se define el marco de referencia que permite la gestión de la protección de datos y de la seguridad de la información en el contexto de las actividades de tratamiento con datos de carácter personal y los sistemas de información de la AEPD.

A su vez, la plena aplicación del Reglamento General de Protección de Datos a partir del 25 de mayo de 2018 exige que la Agencia Española de Protección de Datos adopte una Política de protección de datos a fin de garantizar y poder demostrar que los tratamientos que lleva a cabo son conformes al citado Reglamento.

Por ello, la Agencia ha optado por adoptar una política conjunta de protección de datos y seguridad de la información que permita recoger y delimitar con claridad las responsabilidades y funciones tanto en materia de protección de datos como de seguridad de la información, de forma que se aborden tanto las cuestiones comunes a ambos ámbitos como aquéllas que resultan propias de cada uno de ellos.

La presente Resolución, por tanto, tiene la finalidad de aprobar la política de protección de datos y seguridad de la información de la Agencia Española de Protección de Datos, así como establecer la estructura organizativa para definirla, implantarla y gestionarla, reemplazando a **las resoluciones de la Directora de la Agencia de 10 de mayo de 2018, por la que se aprueba la Política de protección de datos y seguridad de la información** y también a la política de seguridad de la información previamente aprobada por resolución de 15 de junio de 2016.

En su virtud, dispongo:

Artículo 1. *Objeto y ámbito de aplicación*

1. Constituye el objeto de la presente Resolución la aprobación de la política de protección de datos y de seguridad de la información (en adelante PPDSI) en el marco de los sistemas de información y de las actividades de tratamiento con datos de carácter personal de la Agencia Española de Protección de Datos (en adelante AEPD).

2. La PPDSI será de aplicación a todos los sistemas de información y a todas las actividades de tratamiento de datos de carácter personal de los que sea responsable la AEPD.

3. La PPDSI será de obligado cumplimiento para todas las unidades que conforman la estructura de la AEPD y para todo el personal con acceso a la información de la que es responsable aquélla con independencia de su destino, condición laboral o relación por la que se accede a la información.

4. La PPDSI afectará a la información y datos personales tratados por medios electrónicos y en soporte en papel que la AEPD gestiona en el ámbito de sus competencias. Esta información se define según las siguientes normas:

a) Tendrá carácter de información clasificada la que esté afectada por la Ley 9/1968, de 5 de abril, sobre Secretos Oficiales.

b) La información con datos personales estará regulada por 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 –en adelante RGPD-), así como por la Ley Orgánica 3/2018, de 5 de diciembre de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

c) La información contenida en los sistemas de información en el ámbito de la administración electrónica queda regulada por 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.

d) La información producida, conservada o reunida, cualquiera que sea su soporte, susceptible de formar parte del patrimonio documental se verá afectada por el Real Decreto 1164/2002, de 8 de noviembre, por el que se regula la conservación del patrimonio documental con valor histórico, el control de la eliminación de otros documentos de la Administración General del Estado y sus organismos públicos y la conservación de documentos administrativos en soporte distinto al original.

Artículo 2. *Funciones y misión de la AEPD.*

La Agencia Española de Protección de Datos es una autoridad administrativa independiente de ámbito estatal, de las previstas en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, con personalidad jurídica y plena capacidad pública y privada, que actúa con plena independencia de los poderes públicos en el ejercicio de sus funciones.

Su denominación oficial, de conformidad con lo establecido en el artículo 109.3 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, será «Agencia Española de Protección de Datos, Autoridad Administrativa Independiente».
Se relaciona con el Gobierno a través del Ministerio de Justicia.

Corresponde a la Agencia Española de Protección de Datos supervisar la aplicación del Reglamento (UE) 2016/679 y de la Ley Orgánica 3/2018 y, en particular, ejercer las funciones establecidas en el artículo 57 y las potestades previstas en el artículo 58 del RGPD, en la citada ley orgánica y en sus disposiciones de desarrollo. Asimismo, corresponde a la Agencia Española de Protección de Datos el desempeño de las funciones y potestades que le atribuyan otras leyes o normas de Derecho de la Unión Europea.

La AEPD es una autoridad administrativa independiente encargada de supervisar la aplicación del RGPD, con el fin de proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento y de facilitar la libre circulación de datos personales en la Unión. Igualmente contribuirá a la aplicación coherente del RGPD en toda la Unión.

Tiene como objetivos básicos asegurar y facilitar el cumplimiento de la normativa de protección de datos y promover entre los ciudadanos el conocimiento de sus derechos en relación con el tratamiento de sus datos personales y apoyarles en el ejercicio de esos derechos.

Corresponde igualmente a la AEPD la cooperación en materia de protección de datos con las autoridades de control de los Estados miembros de la Unión Europea y las instituciones y organismos de la Unión, especialmente en los términos establecidos en el RGPD, así como con otros organismos internacionales, instituciones, agencias de terceros Estados y la Red Iberoamericana de protección

de Datos. Asimismo, corresponde a la AEPD el control de los datos de carácter personal introducidos en la parte nacional española de la base de datos del Sistema de Información Schengen y el ejercicio de la representación frente a la autoridad de control común de protección de datos del Sistema de Información Schengen.

Artículo 3. *Marco normativo*.

La Agencia Española de Protección de Datos desarrolla sus funciones en el marco normativo de protección de datos, de los procedimientos administrativos y sector público y de la administración electrónica que le resultan de aplicación.

Artículo 4. *Principios de protección de datos y seguridad de la información*

1. La AEPD tratará la información y los datos personales bajo su responsabilidad conforme a los siguientes principios de protección de datos y seguridad de la información:

a) Licitud, lealtad y transparencia: los datos de carácter personal serán tratados de manera lícita, leal y transparente en relación con el interesado;

b) Legitimación en el tratamiento de datos personales: sólo se tratarán los datos de carácter personal cuando dicho tratamiento se encuentre amparado en alguna de las causas de legitimación establecidas en los artículos 6 y 9 del RGPD.

c) Limitación de la finalidad: los datos de carácter personal serán tratados para el cumplimiento de fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines;

d) Minimización de datos: los datos de carácter personal serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados;

e) Exactitud: los datos de carácter personal serán exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan;

f) Limitación del plazo de conservación: los datos de carácter personal personales serán mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines que justificaron su tratamiento;

g) Integridad y confidencialidad: los datos de carácter personal serán tratados de tal manera que se garantice su seguridad, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas. Quienes intervengan en el tratamiento de los datos estarán sujetos al deber de secreto incluso después de haber concluido aquél;

h) Responsabilidad proactiva: la AEPD será responsable del cumplimiento de los principios anteriormente señalados y adoptará las medidas técnicas y organizativas que le permitan estar en condiciones de demostrar dicho cumplimiento;

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

j) 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 pueda estar coordinada e integrada con el resto de iniciativas estratégicas de la AEPD para conformar un todo coherente y eficaz.

k) Responsabilidad diferenciada: En los sistemas de información responsabilidad de la AEPD se observará el principio de responsabilidad diferenciada de forma que se delimiten las diferentes responsabilidades y roles:

i. responsable del tratamiento: determina los fines y medios del tratamiento;

ii. encargado del tratamiento: trata datos personales por cuenta del responsable del tratamiento;

iii. delegado de protección de datos: informa y asesora al responsable del tratamiento de las obligaciones en materia de cumplimiento del RGPD;

iv. responsable de la información: determina los requisitos de seguridad de la información tratada;

v. responsable del servicio: determina los requisitos de seguridad de los servicios prestados;

vi. responsable del sistema: tiene la responsabilidad sobre la prestación de los servicios;

vii. responsable de seguridad de la información: determina las decisiones para satisfacer los requisitos de seguridad.

l) Seguridad integral: La seguridad tenderá a la preservación de la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio. La seguridad se entiende como un proceso integral constituido por todos los elementos

técnicos, humanos, materiales y organizativos, relacionados con el sistema, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural.

m) Gestión de Riesgos: La gestión del riesgo es el conjunto de actividades coordinadas que la AEPD desarrolla para dirigir y controlar el riesgo, entendiendo como riesgo el efecto de la incertidumbre sobre la consecución de los objetivos que, en el marco del RGPD, es la protección de los derechos y libertades de los titulares de los datos que trata la AEPD. El análisis y gestión de riesgos son parte esencial del proceso de protección de datos y de seguridad de la información de la AEPD, de forma que permita el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad. Al evaluar el riesgo la AEPD tendrá en cuenta los riesgos que se derivan para los derechos de las personas con respecto al tratamiento de sus datos personales.

n) Proporcionalidad: La AEPD establecerá medidas de protección, detección y recuperación de forma 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.

o) Proceso de verificación: La AEPD 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.

p) Protección de datos y seguridad desde el diseño: La AEPD promoverá la implantación del principio de protección de datos desde el diseño con el objetivo de cumplir los requisitos definidos en el RGPD y, por tanto, los derechos de los interesados de forma que la protección de datos se encuentre presente en las primeras fases de concepción de un proyecto. Asimismo, la seguridad de la información se aplicará desde el diseño inicial de los sistemas de información

q) Protección de datos por defecto: La AEPD promoverá que los sistemas de información de su titularidad se diseñen y configuren de forma que garanticen la protección de datos por defecto.

2. Las directrices fundamentales de protección de datos y seguridad de la información 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 PPDSI y que inspiran las actuaciones de la AEPD en dicha materia. Se establecen, como mínimos, los siguientes:

a) Registro de actividades de tratamiento y gestión de activos de información: Se mantendrá un registro de actividades de tratamiento, en los términos previstos en el artículo siguiente, que se hará público en la Sede electrónica de la AEPD. Asimismo, los activos de información 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 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.

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.

e) 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.

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 implantarán los mecanismos apropiados para la correcta identificación, registro, resolución y notificación, en los términos previstos en el RGPD, de los incidentes de seguridad.

h) 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.

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

Artículo 5. *Registro de actividades de tratamiento*

La AEPD 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 RGPD.

El registro de actividades de tratamiento se mantendrá continuamente actualizado y podrá consultarse en la página web de la AEPD.

Artículo 6. *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 de carácter personal, se estará igualmente a lo señalado en el artículo siguiente, llevándose a cabo, de forma periódica y al menos cada 2 años, y, en cualquier caso, 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. Esta evaluación incluirá un análisis de los riesgos para los derechos y libertades de las personas físicas respecto de las actividades de tratamiento con datos personales que lleve a cabo la AEPD, así como los sistemas de información que sirven de soporte para dichas actividades de tratamiento.

Asimismo, la AEPD llevará a cabo una evaluación de impacto de las actividades de tratamiento en la protección de datos personales cuando del análisis realizado resulte probable que el tratamiento suponga un riesgo significativo para los derechos y libertades de las personas, conforme a lo previsto en el artículo 35 del RGPD.

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 reevaluación periódica.

El Responsable de Seguridad de la información es el encargado de recomendar un marco de directrices básicas para armonizar los criterios a seguir para la valoración de riesgos.

El Responsable de la Información y los responsables de los Servicios son los propietarios 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.

3. Para el análisis y gestión de riesgos se utilizarán las herramientas disponibles para la Administración General del Estado, así como las guías, recomendaciones y herramientas elaboradas por la AEPD en lo que respecta al tratamiento de datos de carácter personal.

Artículo 7. *Notificación de violaciones de seguridad de los datos de carácter personal*

La AEPD adoptará las medidas necesarias para garantizar la notificación a la propia Agencia Española de Protección de Datos, como autoridad competente, de las violaciones de seguridad de los datos de carácter personal 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 RGPD.

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 RGPD

Artículo 8. *Revisión y auditoría*

La AEPD llevará a cabo de forma periódica, y al menos cada dos años, una auditoría encaminada a la verificación, evaluación y valoración de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad de los tratamientos y sistemas de información.

En todo caso realizará una auditoría específica y extraordinaria cuando se lleven a cabo modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas.

Las auditorías serán supervisadas por el responsable de seguridad de la información y por el delegado de protección de datos.

Artículo 9. *Estructura organizativa*

1. La estructura organizativa para la gestión de la seguridad de la información en el ámbito de la PPDSI de la Agencia Española de Protección de Datos está compuesta por los siguientes agentes:

a) El Comité de Seguridad de la Información.

b) El Responsable de la Información.

c) El Responsable de Seguridad de la información.

d) El Responsable del Servicio.

e) El Responsable del Sistema.

2. La estructura organizativa será competente para mantener, actualizar y hacer cumplir, dentro del ámbito definido por la presente Resolución, la PPDSI de la AEPD.

Artículo 10. *El Comité de Seguridad de la Información*

1. El Comité de Seguridad de la Información, adscrito a la Secretaría General de la AEPD, es un órgano colegiado de los previstos en el artículo 20.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, que gestionará y coordinará todas las actividades relacionadas con la política de protección de datos y la seguridad de los sistemas de información.

2. El Comité de Seguridad está compuesto por los siguientes miembros:

a) El Responsable de seguridad de la información en calidad de coordinador del Comité y que actuará como Secretario;

b) El Jefe de la Unidad de Tecnologías de la Información en calidad de responsable de los sistemas de información con los que se realiza el tratamiento de la información de la que es responsable la Agencia;

c) Un representante de la Secretaría General;

d) Un representante de cada una de las Subdirecciones Generales de la AEPD;

e) Un representante de la Unidad de Apoyo.

g) El delegado de protección de datos participará con voz pero sin voto en las reuniones del Comité de seguridad de la información cuando en el mismo vayan a abordarse cuestiones relacionadas con el tratamiento de datos de carácter personal, así como siempre que se requiera su participación. En todo caso, si un asunto se sometiese a votación se hará constar siempre en acta el parecer del Delegado de Protección de Datos.

3. El Comité de Seguridad de la información actuará en el ámbito del cumplimiento de las medidas a las que se refiere:

a) El Reglamento General de Protección de Datos, así como por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantías de derechos digitales y su normativa de desarrollo.

b) 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, con las modificaciones introducidas por el Real Decreto 951/2015, de 23 de octubre.

4. El Comité de Seguridad de la información coordinará las actividades relacionadas con la seguridad de la información y los sistemas de información ejerciendo las siguientes funciones:

a) Elaborar propuestas de modificación y actualización permanente de la PPDSI de la Agencia y de su estructura organizativa.

b) Establecer criterios para el procedimiento de análisis de riesgos y elaborar propuestas de niveles de riesgos aceptables para seguridad de la información de la Agencia.

c) Aprobar normas y procedimientos para garantizar la seguridad de la información.

d) Promover recursos y medios para la concienciación y formación en materia de seguridad de la información a todo el personal de la Agencia.

e) Velar por el cumplimiento de la PPDSI y su normativa de desarrollo.

f) Analizar los informes facilitados por el Responsable de Seguridad en los que relativos al resultado de los análisis de riesgos, de las auditorías realizadas, de los proyectos y de las iniciativas y acciones de mejora de la seguridad requeridas.

g) Revisar la información aportada por el Responsable de Seguridad de la información relativa a los incidentes de seguridad.

h) Participar en la toma de decisiones que garanticen la seguridad de la información y los servicios de la Agencia.

Artículo 11. *El responsable de la información*

1. La condición de responsable de la información recae en la Dirección de la AEPD que tendrá asimismo la condición de responsable de los tratamientos llevados a cabo por la misma en los términos establecidos en el artículo 4.7 del RGPD.

Corresponde a la Dirección de la Agencia en calidad de máximo responsable aprobar la política de protección de datos y seguridad de la información.

2. En el marco del Esquema Nacional de Seguridad, son funciones del responsable de la información:

a) La aprobación formal de los niveles y medidas de seguridad de la información, a propuesta del Comité de Seguridad de la Información, dentro del marco de lo previsto en los Anexos I y II 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.

b) La aprobación, a propuesta del Comité de Seguridad de la Información, de 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, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, conforme a lo exigido en el RGPD.

Artículo 12. *El responsable de seguridad de la información*

El responsable de seguridad de la información es la persona a la que corresponde la toma de decisiones necesarias para satisfacer los requisitos exigibles para garantizar la seguridad de la información y la seguridad en el tratamiento de datos personales.

Desarrollará su actividad en lo que respecta al cumplimiento de las medidas a las que se refieren:

a) Reglamento General de Protección de Datos, así como por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y su normativa de desarrollo.

b) 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, modificado por el Real Decreto 951/2015, de 23 de octubre.

2. Son funciones del responsable de seguridad de la información de la AEPD las siguientes:

a) Promover la seguridad de la información entre el personal de la Agencia.

b) El mantenimiento de la mejora continua de la seguridad de la información.

c) La elaboración de procedimientos y normativa de seguridad que serán presentados al Comité de Seguridad para su revisión y aprobación.

d) El impulso y la realización de análisis de riesgos sobre los sistemas de información de la Agencia.

e) La elaboración de un informe de revisión anual sobre el estado de la seguridad.

f) Promover la realización de auditorías periódicas internas o externas para verificar el cumplimiento de las obligaciones de la Agencia con relación a la seguridad de la información.

g) La coordinación de las actuaciones en materia de seguridad de la información entre las unidades que explotan la información y los responsables de los servicios de la Agencia.

h) La coordinación con el Centro Criptológico Nacional en la utilización de servicios de respuesta a incidentes de seguridad de la información.

i) La coordinación y control del cumplimiento de las medidas de seguridad definidas en los documentos y normas que desarrollen la presente política.

j) El mantenimiento actualizado del marco documental de la seguridad de la información en el ámbito del Reglamento General de Protección de Datos, así como por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de derechos digitales y su normativa de desarrollo.

k) La gestión de las incidencias de seguridad de la información que se produzcan informando de las más relevantes al Comité de Seguridad y a los responsables de las unidades de la Agencia afectadas por las incidencias.

Artículo 13. *Responsable del servicio*

1. Las funciones de Responsable del Servicio recaerán en la persona titular del órgano o unidad administrativa que gestione cada procedimiento administrativo y en cuyo ámbito se lleve a cabo el tratamiento de los datos de carácter personal, en su caso.

2. El responsable del servicio establecerá, dentro de su ámbito, los requisitos del servicio y los niveles de seguridad del mismo dentro del marco que establece el anexo I del Real Decreto 3/2010, con la colaboración del responsable de seguridad de la información.

Artículo 14. *Responsable del sistema*

La Unidad de Tecnologías de la Información de la AEPD, en calidad de Responsable del Sistema, será el encargado del desarrollo, el funcionamiento y el mantenimiento de los sistemas de información durante su ciclo de vida completo, así como elaborar los procedimientos, guías e instrucciones técnicas que, cumpliendo con lo establecido en la PPDSI, determinan las acciones o tareas a realizar en el desempeño de un proceso.

Artículo 15. *El delegado de protección de datos*

La AEPD cuenta con un delegado de protección de datos, designado por Resolución de la Directora de 3 de noviembre de 2017, a fin de dar cumplimiento a lo requerido en el artículo 37 del RGPD, que llevará a cabo las tareas establecidas en el artículo 39 del citado RGPD, así como las que se deriven de la normativa española de protección de datos de carácter personal y de los documentos de buenas prácticas que se adopten por la propia AEPD, en su condición de autoridad de control, o por el Comité Europeo de Protección de Datos.

En el desempeño de sus tareas el delegado de protección de datos tendrá acceso a los datos personales y procesos de tratamiento.

Artículo 16. *Asignación de tareas*

La Dirección de la Agencia, el Comité de Seguridad, el responsable de seguridad de la información y el delegado de protección de datos podrán, dentro de su respectivo ámbito, asignar tareas relativas a la mejora de los principios recogidos en la presente política a personas o grupos de trabajo. En la asignación de tareas se tendrá en cuenta a todo el personal que presta sus servicios en la Agencia y a especialistas externos cuando sea necesario.

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, en última instancia, a la Dirección, asistida por el Comité de Seguridad de la Información y, cuando proceda, por el delegado de protección de datos, la resolución de conflictos en calidad de máximo responsable de la Agencia.

Artículo 18. *Obligaciones del personal*

Todos los órganos y unidades de la AEPD prestarán su colaboración en las actuaciones de implementación de la Política de protección de datos y seguridad de la información aprobada por esta Resolución.

Todas las personas que presten servicio en la AEPD tienen la obligación de conocer y cumplir lo previsto en la presente Política así como en las normas y procedimientos que la desarrollen.

Todo el personal que presta servicio en la AEPD 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 y aminorando los riesgos a los que se encuentra expuesta la información y los datos personales de los que es titular la Agencia. A tal efecto, comunicarán 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 la AEPD, así como a la difusión entre los mismos de la PPDSI y de su desarrollo normativo.

La Agencia dispondrá 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.

El delegado 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.

Artículo 20. *Desarrollo normativo y revisión de la PPDSI*

1. Corresponderá a la Dirección de la AEPD, a propuesta de los miembros que integran la estructura organizativa de la PPDSI y asistida por el Comité de seguridad de la información y, cuando proceda, por el delegado de protección de datos, la adopción de los procedimientos, guías e instrucciones técnicas necesarios para el desarrollo de la presente Política.

En el proceso de desarrollo normativo podrá requerirse la colaboración de las unidades organizativas que componen la estructura orgánica de la Agencia.

2. La presente PPDSI se someterá a un proceso de revisión, al menos anual, a fin de adaptarse a las circunstancias técnicas u organizativas y evitar su obsolescencia.

Artículo 21. *Relación con otras políticas de la AEPD*

Esta política de protección de datos y seguridad de la información se encontrará alineada con la misión y objetivos establecidos en otras políticas de la Agencia Española de Protección de Datos tales como:

- Código Ético de la AEPD.
- Plan Estratégico de la AEPD.
- Plan de Responsabilidad Social Corporativa de la AEPD
- Política de Calidad de la AEPD.

Disposición adicional única. *Publicidad*

La presente Resolución se publicará en la sede electrónica de la AEPD.

Disposición derogatoria única. *Derogación normativa*

Quedan derogadas las resoluciones de la Directora de la Agencia de 10 de mayo de 2018 por la que se aprueba la Política de protección de datos y seguridad de la información de la Agencia Española de Protección de datos, y la resolución de 15 de junio de 2016, por la que se aprueba la política de seguridad de la información de la AEPD.

Disposición final única. *Entrada en vigor*

Esta Resolución entrará en vigor el día de su publicación en la Sede Electrónica de la AEPD.