3. Otras disposiciones

CONSEJERÍA DE LA PRESIDENCIA, INTERIOR, DIÁLOGO SOCIAL Y SIMPLIFICACIÓN ADMINISTRATIVA

Resolución de 12 de julio de 2024, de la Dirección Gerencia de la Agencia Digital de Andalucía, por la que se aprueba la Política de Seguridad Interior, Seguridad de las Tecnologías de la Información y las Telecomunicaciones (TIC) y Protección de Datos de la Agencia Digital de Andalucía.

Visto el expediente tramitado en la Secretaría General y en la Dirección General de Estrategia Digital, relativo a la Política de Seguridad Interior, Seguridad de las Tecnologías de la Información y las Telecomunicaciones (TIC) y Protección de Datos, y en atención a los siguientes

ANTECEDENTES DE HECHO

La Administración de la Junta de Andalucía mediante el Decreto 1/2011, de 11 de enero, modificado por el Decreto 70/2017, de 6 de junio, aprobó la Política de Seguridad de las Tecnologías de la Información y Comunicaciones en la Administración de la Junta de Andalucía, disponiendo que las distintas Consejerías y demás entidades deberán disponer formalmente de su propias normas específicas de política de seguridad TIC, y adecuar, en su caso, las directrices comunes de la Administración de la Junta de Andalucía a sus particularidades. Asimismo, cada Consejería y entidad deberá contar con un Comité de Seguridad de las Tecnologías de la Información y Comunicación (en adelante TIC), que actuará como órgano de dirección y seguimiento en materia de seguridad y demás perfiles previstos en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante ENS).

El ENS se encuentra establecido en el artículo 156.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, regulado por el Real Decreto 311/2022, de 3 de mayo, y está constituido por los principios básicos y requisitos mínimos necesarios para una protección adecuada de la información tratada y los servicios prestados por las entidades de su ámbito de aplicación, con objeto de asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos que gestionen en el ejercicio de sus competencias.

Su finalidad última es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas dirigidas a garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permitan a la ciudadanía y a las Administraciones Públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios. En este contexto, el ENS exige que todo el sector público cuente con una política de seguridad formalmente aprobada por el órgano competente que ostente las máximas competencias ejecutivas.

FUNDAMENTOS DE DERECHO

El Decreto 171/2020, de 13 de octubre, por el que se establece la Política de Seguridad Interior en la Administración de la Junta de Andalucía, define un completo sistema de prevención y reacción ante daños en las personas, el patrimonio y el funcionamiento, intencionadamente provocados por agentes externos, personal propio o personas usuarias.

00305160

El citado decreto regula un modelo organizativo funcional en el que por simplificación, eficacia y eficiencia se ha evitado la creación de un Comité de Seguridad Interior, optando por incluir las que hubieran sido sus funciones y tareas entre las de los ya existentes comités de seguridad TIC. En este sentido, en su disposición final primera, modifica el reseñado Decreto 1/2011, de 11 de enero, indicando que: «Todas las alusiones en el texto a los «Comités de Seguridad TIC de las entidades» quedan sustituidas por Comités de Seguridad Interior y Seguridad TIC de las Consejerías o entidades dependientes singulares». Asimismo, el artículo 9 del Decreto 171/2020, de 13 de octubre, determina, respecto a las normas de creación de dichos Comités, que «modificarán su denominación añadiendo su definición como órganos de dirección y seguimiento en materia de seguridad interior y actualizando, de ser necesario, su composición y régimen de los mismos, con descripción incluso, de las nuevas funciones a incorporar». Por su parte, su artículo 10.1 establece que: «Partiendo de sus propios recursos directos, en cada una de las Consejerías y en aquellas de sus entidades dependientes en las que éstas lo consideren necesario por virtud del volumen o singularidad de los activos, se contará con una Unidad de Seguridad Interior que ejerza la responsabilidad ejecutiva para la seguridad interior del conjunto de los activos en su ámbito, debiendo ser designada por el Comité de Seguridad Interior y Seguridad TIC». Asimismo, el párrafo 2 del citado precepto continúa disponiendo que la composición, atribuciones, funcionamiento y método de trabajo del Comité de Seguridad TIC deberá ser aprobada por el máximo órgano de dirección de la entidad.

Por su parte, la aplicación de la normativa sobre protección de datos de carácter personal supone para la Agencia Digital de Andalucía, en tanto responsable y también encargada de tratamientos de esta naturaleza según lo dispuesto en la disposición adicional cuarta del Decreto 128/2021, de 30 de marzo, por el que se aprueban los Estatutos de la Agencia Digital de Andalucía, la necesaria adopción de una serie de medidas de carácter técnico y organizativo tendentes a garantizar los derechos de los titulares de dichos datos personales. Por ello, en la elaboración de esta resolución se han tenido en cuenta el Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante RGPD), directamente aplicable a partir del 25 de mayo de 2018, y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD).

La disposición adicional primera de la LOPDGDD determina que los responsables enumerados en el artículo 77.1 de la citada ley, deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el ENS. Por su parte, la normativa reguladora del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, en su artículo 3 establece que cuando un sistema de información trate datos personales le será de aplicación lo dispuesto en el RGPD y en la LOPDGDD, o, en su caso, la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, el resto de normativa de aplicación, así como los criterios que se establezcan por la Agencia Española de Protección de Datos o en su ámbito competencial, por las autoridades autonómicas de protección de datos.

En consecuencia, la convergencia de los requisitos de seguridad interior, los referidos requisitos sobre los sistemas de información, y los exigidos para la protección de datos de carácter personal hacen aconsejable no acometer acciones desagregadas, que atiendan a cada dimensión por separado, pues ello podría provocar duplicidades, antinomias, confusión y descoordinación internas, además de resultar más oneroso desde el punto de vista de la inversión de recursos humanos, económicos, técnicos y organizativos.

00305160

También se ha tenido en cuenta la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, conocida como «Directiva NIS», así como su transposición al ordenamiento jurídico español mediante el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

En resumen, todos los preceptos legales anteriores justifican la adopción de una Política de Seguridad de la Agencia Digital de Andalucía integrada, así como un único Comité de Seguridad Interior, Seguridad TIC y Protección de Datos.

En su virtud, en uso de las atribuciones conferidas por los artículos 44.2 de la Ley 6/2006, de 24 de octubre, del Gobierno de la Comunidad Autónoma de Andalucía, y 26.2.a) de la Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía, de conformidad con lo establecido en el artículo 14 de los Estatutos de la Agencia Digital de Andalucía, aprobado por el Decreto 128/2021, de 30 de marzo, y a propuesta de las personas titulares de la Secretaría General y de la Dirección General de Estrategia Digital,

R E S U E L V O

Primero. Aprobar la Política de Seguridad Interior, Seguridad de las Tecnologías de la Información y Telecomunicaciones (TIC) y Protección de Datos de la Agencia Digital de Andalucía, en los términos que se especifican en anexo a esta resolución.

Segundo. Publicar el texto en el Portal Web de la Agencia Digital de Andalucía, así como en el Portal de Transparencia de la Agencia Digital de Andalucía.

Tercero. Ordenar la publicación de la presente resolución en el Boletín Oficial de la Junta de Andalucía.

Cuarto. La presente resolución surtirá efectos desde el día siguiente al de su aprobación.

Sevilla, 12 de julio de 2024.- El Director Gerente, Raúl Jiménez Jiménez.

A N E X O

POLÍTICA DE SEGURIDAD INTERIOR, SEGURIDAD TIC Y PROTECCIÓN DE DATOS DE LA AGENCIA DIGITAL DE ANDALUCÍA

Primero. Disposiciones generales.

1. Objeto.

El presente documento tiene por objeto establecer la Política de Seguridad Interior, Seguridad TIC y Protección de Datos (en adelante, la Política) de la Agencia Digital de Andalucía (en adelante, la Agencia), y el marco organizativo y tecnológico de acuerdo con la normativa reguladora de la Política de Seguridad Interior en la Administración de la Junta de Andalucía, la legislación de seguridad de las tecnologías de la información y comunicaciones de la Administración de la Junta de Andalucía, en cumplimiento de la normativa reguladora del Esquema Nacional de Seguridad (en adelante, ENS) y de las disposiciones de protección de datos.

2. Ámbito de aplicación.

En materia de Seguridad TIC, esta Política de Seguridad se aplicará a todos los sistemas de información que son responsabilidad de la Agencia para el ejercicio de las competencias que tiene atribuidas, en concreto, en aquellos sistemas de información

00305160

cuyo Responsable de la Información o Responsable del Servicio (en el sentido de los artículos 11 y 13 del Real Decreto 311/2022) es empleado público de la Agencia.

En materia de Protección de Datos, se aplicará a los tratamientos de datos personales total o parcialmente automatizados, así como los tratamientos no automatizados de datos personales contenidos o destinados a ser incluidos en ficheros de la Agencia, como responsable o encargada de tratamientos.

En materia de Seguridad Interior, la Política se aplicará a los activos que son titularidad de la Agencia.

Lo dispuesto en la Política deberá ser observado por todos los empleados públicos de la Agencia, así como por aquellas personas que tengan acceso a sus sistemas de información y a los tratamientos de datos personales que en ellos se gestionan.

La presente disposición se aplica a todas las unidades administrativas de la Agencia. Los entes y organismos públicos adscritos a la Agencia adoptarán su propia Política de Seguridad que deberá adecuarse, con sus peculiaridades específicas, a las presentes prescripciones.

Segundo. Objetivos, principios, definiciones y marco regulador.

1. Objetivos, principios y definiciones.

1. Se definen los siguientes principios rectores.

a) Seguridad coordinada y estructurada.

La seguridad de los sistemas de información se abordará aplicando de forma coherente y coordinada esta Política, las normas que la desarrollen y el referente legislativo del ENS a cualquier tipo de información tratada en dichos sistemas, atendiendo a la previsión que en materia de seguridad de los datos personales contiene la disposición adicional primera de la LOPDGDD.

De igual forma, a la hora de ejecutar las actividades de la seguridad de la información se respetarán los principios de competencia y separación de funciones, conforme a las atribuciones conferidas a cada componente de la estructura de organización de la seguridad y de la protección de datos personales.

b) Acceso a la información.

Los derechos de acceso de las personas usuarias a la información se regirán por los siguientes principios:

b.1. Mínimo privilegio. Los privilegios de cada persona se reducirán al mínimo estrictamente necesario para cumplir sus obligaciones.

b.2. Necesidad de conocer. Los privilegios se limitarán de forma que las personas sólo accederán al conocimiento de aquella información requerida para cumplir sus obligaciones.

b.3. Capacidad de autorizar. Sólo y exclusivamente las personas con competencia para ello podrá conceder, alterar o anular la autorización de acceso a los recursos, conforme a los criterios establecidos por su responsable.

c) Ciclo vital de la información.

La seguridad y la protección de los datos de carácter personal estarán presentes durante todo el ciclo de vida.

d) Deber de secreto.

Las personas usuarias están obligadas a guardar secreto profesional de toda aquella información de la que tengan conocimiento con ocasión del ejercicio de su cargo o actividad profesional. Esta obligación se mantendrá incluso después de haber finalizado la relación con la Agencia.

El deber de confidencialidad y secreto profesional se establecerá de forma expresa en todo tipo de relaciones –administrativas, civiles o mercantiles-, que impliquen o supongan acceso o tratamiento de la información, incluidos los servicios de simple alojamiento, transporte o soporte técnico.

00305160

2. En lo referente a Seguridad TIC, se adoptan los principios, objetivos y definiciones establecidos en los artículos 2, 4 y 5 del Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía, así como los principios básicos y requisitos mínimos establecidos en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

3. En lo relativo a Seguridad Interior, se adoptan los objetivos, definiciones y principios definidos en los artículos 3, 4 y 5 del Decreto 171/2020, de 13 de octubre, por el que se establece la Política de Seguridad Interior en la Administración de la Junta de Andalucía.

4. En lo concerniente a Protección de Datos se adoptan igualmente los objetivos, definiciones y principios establecidos en los artículos 1, 4, 5, 6, 7, 8, 9 y 10 del RGPD y los recogidos en los artículos 4, 5, 6, 7, 8, 9, 10 de la LOPDGDD.

Asimismo, según los principios aplicados al tratamiento, los datos personales serán tratados de manera lícita, leal y transparente, recogidos con fines determinados, explícitos y legítimos, y no tratados ulteriormente de manera incompatible con dichos fines. Los datos serán adecuados, pertinentes y limitados (principio de minimización), exactos y actualizados, mantenidos durante no más tiempo del necesario para los fines del tratamiento, y tratados de manera que se garantice una seguridad adecuada incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas y organizativas adecuadas (integridad y confidencialidad).

El principio de transparencia por su parte (artículo 12.º del RGPD) exige además el deber al responsable de tomar medidas oportunas para facilitar al interesado toda información relativa a sus tratamientos, sus ejercicios de derechos o violaciones de seguridad en un lenguaje sencillo claro, de forma concisa, transparente, inteligible y de fácil acceso.

El responsable del tratamiento además queda obligado al cumplimiento de los principios y derechos anteriores y a su acreditación.

2. Marco regulador.

La presente resolución, con independencia de la legislación complementaria de aplicación, está basada en la siguiente normativa:

• Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía (BOJA número 11, de 18 de enero de 2011).

• Decreto 70/2017, de 6 de junio, por el que se modifica el Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía (BOJA número 110, de 12 de junio de 2017).

• Decreto 171/2020, de 13 de octubre, por el que se establece la Política de Seguridad Interior en la Administración de la Junta de Andalucía (BOJA número 201, de 16 de octubre de 2020).

• Decreto 128/2021, de 30 de marzo, por el que se aprueban los Estatutos de la Agencia Digital de Andalucía (BOJA número 65, de 8 de abril de 2021).

• Decreto 572/2022, de 27 de diciembre, por el que se modifica el Decreto 152/2022, de 9 de agosto, por el que se establece la estructura orgánica de la Consejería de la Presidencia, Interior, Diálogo Social y Simplificación Administrativa; el Decreto 128/2021, de 30 de marzo, por el que se aprueban los Estatutos de la Agencia Digital de Andalucía; el Decreto 226/2020, de 29 de diciembre, por el que se regula la organización territorial provincial de la Administración de la Junta de Andalucía, y el Decreto 289/2015, de 21 de julio, por el que se regula la organización administrativa en materia de transparencia pública en el ámbito de la Administración de la Junta de Andalucía y sus entidades instrumentales (BOJA número 249, de 30 de diciembre de 2022).

• Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (BOE número 106, de 4 de mayo de 2022).

00305160

• Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

• Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

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

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

• Resolución de 22 de octubre de 2020, de la Secretaría General para la Administración Pública, por la que se aprueba el Código de Conducta en el uso de las Tecnologías de la Información y la Comunicación para profesionales públicos de la Administración de la Junta de Andalucía (BOJA número 208, de 27 de octubre de 2020).

• 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).

Tercero. Organización de la seguridad.

1. Estructura organizativa.

En el ámbito de la Agencia, además de las atribuciones directamente relacionadas con la Seguridad TIC existen otras relacionadas con las normativas de seguridad interior, protección de datos personales, protección de infraestructuras críticas y servicios esenciales. La estructura organizativa mínima para la gestión de estas responsabilidades será la siguiente:

a) El Comité de Seguridad Interior, Seguridad TIC y Protección de Datos de la Agencia, en adelante el Comité.

b) La persona Responsable de Seguridad TIC.

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

d) Las personas Responsables de los Sistemas.

e) La persona Responsable de la Unidad de Seguridad Interior (artículo 10 del Decreto 171/2020, de 13 de octubre).

f) El Responsable de los Tratamientos de datos personales (artículo 4 del RGPD).

g) El Encargado de los Tratamientos de datos personales de otros organismos (artículo 4.8 del RGPD).

h) La persona Delegada de Protección de Datos, en adelante DPD.

i) La persona Responsable de Seguridad y Enlace y las personas Delegadas de Seguridad de las infraestructuras críticas según lo descrito por el Real Decreto 704/2011, de 20 de mayo.

j) La persona, unidad u órgano Responsable de la Seguridad de la Información, según lo descrito en el Real Decreto 43/2021, de 26 de enero.

2. Comité de Seguridad Interior, Seguridad TIC y Protección de Datos.

1. Se crea el Comité de Seguridad Interior, Seguridad TIC y Protección de Datos de la Agencia Digital de Andalucía. El Comité actuará como órgano de dirección y seguimiento en las tres materias, así como en los ámbitos de protección de Infraestructuras Críticas y de Servicios Esenciales.
2. En el ámbito de la seguridad interior, el Comité tendrá asignadas las siguientes funciones:

a) La definición, aprobación y seguimiento de los objetivos, iniciativas y planes estratégicos para la seguridad interior, incluido el Plan de Seguridad Interior.

b) Velar por la disponibilidad de los recursos necesarios para desarrollar las iniciativas y planes estratégicos definidos.

c) El establecimiento de directrices comunes y la supervisión del cumplimiento de la normativa de seguridad interior.

00305160

d) La aprobación del modelo de relación con los Puntos Coordinadores de Seguridad Interior.

e) La promoción de la educación, el entrenamiento y la concienciación sobre las medidas relativas a la seguridad interior entre el personal.

f) El análisis y la adopción de decisiones en la respuesta a incidentes susceptibles de generar una crisis de seguridad interior.

g) La designación del Responsable de Seguridad Interior.

3. En el ámbito de la seguridad TIC y protección de datos, el Comité tendrá asignadas las siguientes funciones:

a) Proponer, para su aprobación, el desarrollo de la Política de Seguridad TIC, de las Políticas de Protección de datos de obligado cumplimiento, y de los instrumentos necesarios como puedan ser Comités Técnicos, directrices y normas para su desarrollo.

b) Velar por la concienciación y formación del personal en materia de Seguridad TIC y protección de datos.

c) Planificar y priorizar las iniciativas necesarias para cumplir con las directrices, los objetivos y los principios básicos de seguridad TIC y de protección de datos marcados en la presente política de Seguridad.

d) Proporcionar los medios y recursos necesarios para posibilitar la realización de las iniciativas planificadas.

e) Coordinar a alto nivel todas las actuaciones de seguridad, velando porque la definición y el desarrollo de estas se adecuen en todo momento a las directrices marcadas en esta Política, involucrando a las diferentes áreas implicadas.

f) Velar porque todos los ámbitos de responsabilidad y actuación en relación con la Seguridad TIC y protección de datos queden perfectamente definidos, aprobando los nombramientos necesarios para ello. Especialmente, para asegurar que todas y cada una de las personas miembros de la estructura de seguridad definida, conozcan sus funciones y responsabilidades.

g) Velar porque la Seguridad TIC y la protección de datos se tengan en cuenta en todos los proyectos, desde su especificación inicial (fase de diseño) y durante todo su ciclo de vida. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas de información TIC de cualquier naturaleza incluidos aquellos que traten datos personales.

h) Asegurar que el desarrollo normativo que tenga incidencia en el desarrollo o explotación de sistemas de información se adecua a lo establecido en la política de Seguridad TIC y Protección de Datos.

i) Resolver los conflictos que puedan aparecer entre las diferentes personas responsables o entre diferentes unidades de la organización en materia de Seguridad TIC y protección de datos.

j) Coordinar las medidas técnicas y organizativas establecidas en la normativa de protección de datos personales, de acuerdo con los correspondientes análisis de riesgos para los derechos y libertades y, en su caso, las evaluaciones de impacto en la protección de datos, contando con el asesoramiento del DPD.

k) Conocer la situación en materia de protección de infraestructuras críticas y de servicios esenciales y velar por el cumplimiento de la normativa asociada.

l) Designar al Responsable de Seguridad TIC, que será nombrado por resolución de la Dirección Gerencia, contemplando la diferenciación de responsabilidades dictada por los artículos 11 y 13.3 del ENS.

m) Realizar la revisión de esta Política con periodicidad mínima anual, para valorar su vigencia o la necesidad de actualización en base a nuevos riesgos aparecidos o nuevas necesidades de garantizar la seguridad de la información.

n) Elevar las propuestas de revisión de esta Política a su aprobación por la Dirección Gerencia de la Agencia.

00305160

4. El Comité estará compuesto por los siguientes miembros:

a) Presidencia: La persona titular de la Dirección Gerencia.

b) Vicepresidencia: La persona titular de la Dirección General de Estrategia Digital.

c) Vocalías: Las personas titulares de las Subdirecciones y la persona titular de la Secretaría General de la Agencia.

d) Secretaría: La persona responsable de Seguridad TIC.

e) La persona que ostente la condición de Delegado de Protección de Datos, la persona titular de la Unidad de Seguridad Interior y las personas Responsables de Sistemas asistirán en calidad de asesores a las reuniones del Comité. Las personas Responsables de los Sistemas podrán ser representadas por las personas titulares de las unidades a las que pertenecen.

f) Las personas que ostenten la condición de Responsable de Seguridad y Enlace (en el ámbito de infraestructuras críticas) y de Responsable de la seguridad de la información (en el ámbito de los servicios esenciales), si son distintas de las anteriormente convocadas.

El Comité podrá convocar a sus reuniones a las personas que en cada caso autorice la Presidencia, por propia iniciativa o a propuesta de alguno de sus miembros. Asimismo, podrá recabar de personal técnico especializado, propio o externo, la información pertinente para la toma de decisiones.

En caso de vacante, ausencia, enfermedad u otras causas legales:

• la Presidencia será sustituida por la persona titular de la Vicepresidencia.

• la Secretaría será sustituida por el Jefe del Servicio de Ciberseguridad de la Agencia.

Las vocalías podrán ser sustituidas por una persona designada por la Presidencia entre personal funcionario que ocupen puestos de trabajo de nivel 28 o superior.

En la composición del Comité ha de garantizarse, en la medida de lo posible, la representación paritaria de mujeres y hombres, conforme a lo establecido en el artículo 19.2 de la Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía, y a la definición de representación equilibrada contenida en el artículo 3.3 de la Ley 12/2007, de 26 de noviembre, para la Promoción de la Igualdad de Género en Andalucía.

5. El Comité se reunirá con carácter ordinario una vez al año, y con carácter extraordinario por acuerdo de la Presidencia, a iniciativa propia o previa solicitud razonada de uno de sus miembros.
6. El Comité se podrá constituir, convocar, celebrar sus sesiones, adoptar acuerdos y remitir actas, tanto de forma presencial como utilizando redes de comunicación a distancia, con las medidas adecuadas que garanticen la identidad de las personas comunicantes y la autenticidad de la información entre ellas transmitida, de conformidad con lo establecido en el artículo 91.3 de la reseñada Ley 9/2007, de 22 de octubre.
7. La presidencia del Comité ostentará voto de calidad en caso de empate en la toma de decisiones.
8. De todas las sesiones celebradas se levantará un acta con los acuerdos adoptados. Esta acta tendrá carácter de información reservada dada la naturaleza de las funciones y los contenidos a tratar por el Comité.
9. El Comité se regirá por este documento, por la normativa reguladora de la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía, por la Política de Seguridad Interior en la Administración de la Junta de Andalucía, así como lo dispuesto para los órganos colegiados en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, y por el resto de normativa aplicable, como la reguladora del ENS y la normativa de protección de datos personales.
10. La primera reunión del Comité se celebrará en un plazo máximo de tres meses a partir de la entrada en vigor de la presente resolución, debiéndose haber realizado

00305160

con carácter previo los nombramientos de Responsable de Seguridad y Enlace (en el ámbito de infraestructuras críticas) y de Responsable de la seguridad de la información (en el ámbito de los servicios esenciales).

11. En la primera reunión del Comité se designará a las personas responsables de Seguridad TIC y de Seguridad Interior, quienes deberán estar presentes y comenzar con el ejercicio de su cargo.

3. Responsable de seguridad TIC.

1. De acuerdo con lo establecido en el artículo 13.2.c del Real Decreto 311/2022, de 3 de mayo (Esquema Nacional de Seguridad), y en el artículo 11 del Decreto 1/2011, de 11 de enero (Política de Seguridad TIC en la Administración de la Junta de Andalucía, modificado por el Decreto 70/2017, de 6 de junio), la Agencia contará con un Responsable de Seguridad TIC, garantizando el principio de función diferenciada, que ejerza las funciones de Responsabilidad de Seguridad TIC de la Agencia, debiendo ser designada la persona responsable por el Comité. Su nombramiento se realizará por resolución de la Dirección Gerencia.

2. El Responsable de Seguridad TIC tendrá las siguientes atribuciones:

a) Soporte técnico, asesoramiento e información al Comité, así como de ejecución de las decisiones y acuerdos adoptados por éste.

b) Diseño y ejecución de los programas de actuación propios de la Agencia, incluyendo, entre otros, planes directores de seguridad, proyectos de desarrollo normativo, auditorías de cumplimiento y planes de adecuación legal.

c) Delimitación, implantación y mantenimiento de los controles de carácter organizativo para la protección de los datos, aplicaciones y sistemas, así como la realización y mantenimiento de los análisis de riesgos.

d) Supervisión sistemática de los controles de carácter procedimental, operacional y medidas técnicas de protección de los datos, aplicaciones y sistemas de la Agencia.

e) Determinación y supervisión de los criterios y requisitos técnicos de seguridad aplicados en las distintas fases del ciclo de vida de los soportes, sistemas y aplicaciones de la Agencia por parte de los Servicios o unidades responsables de la prestación de los servicios de tecnologías de la información y comunicaciones. Antes de la puesta en producción de nuevos sistemas de información o evolutivos de los existentes, el Responsable de Seguridad TIC deberá evaluar los aspectos de seguridad y comunicar los posibles riesgos a la persona responsable de la Información y a la persona responsable del Servicio.

f) Definición y ejecución de los programas formativos y de concienciación relacionados con buenas prácticas de seguridad TIC en el ámbito de la Agencia, procurando promover, en el proceso de selección de las personas participantes en estos programas, la concurrencia de mujeres.

g) Aplicación de los criterios y directrices de gestión de la seguridad TIC emanadas de la Unidad de Seguridad TIC Corporativa.

h) Cuantas otras le sean encomendadas por el órgano directivo de la Agencia del que dependa funcional u orgánicamente.

3. El responsable de seguridad TIC elaborará y mantendrá un inventario de servicios y sistemas en el que se indiquen expresamente las personas u órganos nombrados por el comité, que asumen las figuras de responsable de la información, responsable del servicio, y responsable del sistema. En aquellos servicios y sistemas que traten datos de carácter personal y en coordinación con el DPD, deberán ser identificados los tratamientos de datos personales realizados por o encomendados a la Agencia, y las unidades administrativas u organismos que asumen las figuras de responsable del tratamiento y encargado del tratamiento.

4. Responsables de la Información y de los Servicios.

1. Las personas Responsables de la Información serán las personas titulares de las Subdirecciones en las que se estructura la Dirección General de Estrategia Digital, y la

00305160

persona titular de la Secretaría General, quienes deciden sobre la finalidad, contenido y uso de la información de cada sistema de información.

2. Las personas Responsables del Servicio serán las personas titulares de las Subdirecciones en las que se estructura la Dirección General de Estrategia Digital, y la persona titular de la Secretaría General, quienes deciden sobre las características del servicio a prestar por cada sistema de información.

3. Las funciones de los responsables de la información y de los servicios serán las siguientes:

a) Asistir a la determinación de los requisitos de seguridad TIC, categorizando la información/los servicios mediante la valoración de los impactos de los incidentes que puedan producirse.

b) Proporcionar la información necesaria al Responsable de Seguridad TIC para realizar los preceptivos análisis de riesgos TIC, con la finalidad de establecer las salvaguardas a implantar. Para ello contarán con la colaboración de las personas responsables de los Sistemas.

c) Verificar que los análisis de riesgos realizados se corresponden en todo momento con la información aportada para la realización de éstos.

d) Aceptar los riesgos residuales de las informaciones tratadas y los servicios prestados, identificados en el análisis de riesgos y realizar su seguimiento y control.

5. Responsables de los tratamientos de datos personales.

1. El Responsable del Tratamiento será quien determine los fines y los elementos esenciales de los medios del tratamiento.

Por elementos esenciales se entiende los medios estrechamente ligados al fin y el alcance del tratamiento; como el tipo de datos personales tratados, la duración del tratamiento, las categorías de destinatarios y las categorías de interesados. Además de estar relacionados con el fin del tratamiento, los medios esenciales se encuentran estrechamente vinculados a la cuestión de licitud, necesidad y proporcionalidad. Y a su vez, los medios no esenciales están relacionados con aspectos prácticos del tratamiento en sí, como la elección de la infraestructura tecnológica en materia de informática y telecomunicaciones, o las aplicaciones informáticas que tratan estos datos, o la decisión sobre los pormenores de las medidas de seguridad, que suelen depender del encargado del tratamiento.

2. Las funciones y responsabilidades de la Agencia, para aquellos tratamientos en los que actúa como responsable del tratamiento, son las siguientes:

a) Garantizar el cumplimiento de las políticas, normativas y procedimientos aprobados e implementados en la Agencia en materia de protección de datos.

b) Velar por el cumplimiento de los principios relativos al tratamiento, el derecho de información de las personas interesadas, y el ejercicio y atención a las solicitudes en el ejercicio de sus derechos.

c) Aplicar medidas técnicas y organizativas apropiadas a fin de garantizar y acreditar que el tratamiento es conforme con el RGPD teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas (Responsabilidad proactiva y análisis y gestión del riesgo).

d) Aplicar medidas técnicas y organizativas para aplicar la privacidad desde el diseño y por defecto y la seguridad del tratamiento de datos personales para preservar un nivel de seguridad adecuado al riesgo.

e) Llevar un registro de actividades de tratamiento de datos de carácter personal bajo su responsabilidad y de acuerdo con lo establecido en el artículo 30.1 del Reglamento. Las propuestas de inclusión del tratamiento deberán ser comunicadas al DPD antes de cualquier operación.

00305160

f) En caso de violación de la seguridad de los datos personales, el Responsable del Tratamiento la notificará a la autoridad de control competente sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos justificativos de la dilación. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el Responsable del Tratamiento la comunicará al interesado sin dilación indebida. Dicha notificación y comunicación se atendrán a lo establecido en los artículos 33 y 34 del Reglamento y el resto de normativa de datos de carácter personal aplicable.

g) Aprobar los preceptivos análisis de riesgos para los derechos y libertades de las personas físicas, identificando y evaluando los factores de riesgos relacionados con las finalidades de los tratamientos, los tipos de datos utilizados, la extensión y alcance del tratamiento, las categorías de las personas interesadas, los factores técnicos del tratamiento, la recogida y generación de los datos, los efectos colaterales del tratamiento, la categoría del responsable o encargado del tratamiento y los riesgos que se derivan de la posible materialización de brechas de seguridad sobre datos personales, asegurando que toda la metodología de la gestión del riesgo quede documentada.

h) Evaluar la obligación y necesidad de realizar una evaluación de impacto en protección de datos.

i) Identificar las medidas de control de riesgos sobre el concepto y diseño del tratamiento, las de gobernanza y políticas de protección de datos, las de protección de datos desde el diseño de las operaciones del tratamiento, y las medidas de gestión de brechas de datos personales y seguridad para los derechos y libertades de las personas físicas.

j) Realizar y aprobar antes del inicio del tratamiento, la evaluación de impacto en aquellos casos en los que la evaluación hubiera dado positiva, incluyendo en la misma el juicio de idoneidad, necesidad y proporcionalidad del tratamiento.

k) Elaborar en los expedientes de proyectos normativos que afecten a la protección de los datos personales y en los casos en que corresponda, el informe preceptivo para la Comisión Consultiva del Consejo de Transparencia y Protección de Datos de Andalucía, que conformará una «Memoria relativa a la protección de datos», bien como documento autónomo o bien integrado en la «Memoria de Análisis de Impacto Normativo» (MAIN).

l) Redactar el análisis del impacto sobre la protección de los datos personales en la elaboración de los expedientes que deberán formar parte de la MAIN.

m) Diseñar y ejecutar los planes de acción con los controles y garantías identificados en el análisis de riesgos y realizar su seguimiento y control.

n) Aceptar los riesgos residuales identificados en el análisis de riesgos para los derechos y libertades de los interesados y realizar su seguimiento y control.

ñ) La designación del encargado de tratamiento recaerá en aquellos empleados públicos que ofrezcan garantías suficientes para aplicar las medidas técnicas y organizativas apropiadas para que el tratamiento sea conforme al RGPD y garantice la protección de los derechos de las personas interesadas, de conformidad con el artículo 28 del reglamento.

o) Respaldar al delegado de protección de datos en el desempeño de las funciones mencionadas en el artículo 39, facilitando los recursos necesarios para el desempeño de dichas funciones y el acceso a los datos personales y a las operaciones de tratamiento, y para el mantenimiento de sus conocimientos especializados.

p) Asegurar la participación y asesoramiento del delegado de protección de datos desde el principio de la elaboración de cualquier proyecto de disposición normativa que pueda afectar el derecho de protección de datos y en el proceso de elaboración del análisis del impacto.

00305160

3. Las responsabilidades operativas de la Agencia en su condición de responsable, recaen en los titulares que ostentan las Subdirecciones y la Secretaría General de la Agencia. Será la persona titular de la Dirección General de Estrategia Digital quien las asuma cuando los tratamientos afecten a más de uno de los titulares anteriores mencionados.

6. La Agencia como Encargada de los tratamientos de datos personales.

1. Cuando la Agencia, en el ejercicio de sus fines y funciones, trate datos personales cuyo responsable del tratamiento esté comprendido en el ámbito del apartado 2 del artículo 6 de sus Estatutos, se considerará que actúa como encargado del tratamiento, de conformidad con lo establecido en el apartado 5 del artículo 33 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
2. Cada Consejería, Agencia administrativa o de régimen especial para la cual la Agencia Digital de Andalucía desarrolle sus fines de definición y ejecución de los instrumentos de tecnologías de la información, telecomunicaciones, ciberseguridad y gobierno abierto y su estrategia digital, ha de ser considerada como responsable, ya que ejercerá la dirección funcional de los sistemas de información sobre las materias de su competencia, así como la formulación y priorización de las necesidades en materia de tecnologías de la información y la comunicación, a través de los instrumentos y medios organizativos o de otra índole que apruebe. Todo ello, en virtud de la disposición adicional tercera de los Estatutos de la Agencia.
3. Cuando la Agencia actúa en interés de estos responsables, puede identificar los medios no esenciales de las operaciones del tratamiento que se utilizarán o las medidas técnicas y organizativas que puedan ser necesarias, colaborando con los responsables del tratamiento en el cumplimiento de sus obligaciones en materia de protección de datos.
4. A pesar de que las decisiones sobre los medios no esenciales pueden desarrollarse desde la Agencia, los responsables por su parte deberán determinar las medidas técnicas y organizativas adecuadas para garantizar una protección de datos desde el diseño y por defecto, a tenor del artículo 25 del RGPD, y los requisitos de seguridad del tratamiento, en función del artículo 32 del RGPD.

En todo caso, los responsables del tratamiento continúan siendo responsables de la aplicación de las medidas técnicas y organizativas apropiadas a fin de garantizar y acreditar que el tratamiento es conforme con el Reglamento (artículo 24).

5. Como encargado del tratamiento, la Agencia deberá llevar un registro de actividades de tratamiento de datos de carácter personal bajo su responsabilidad y de acuerdo con lo establecido en el artículo 30.2 del Reglamento. Las propuestas de inclusión del tratamiento en este registro de actividades deberán ser comunicadas al DPD antes de cualquier operación.
6. El objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados serán los que se especifiquen en el correspondiente registro de actividades de tratamiento de cada responsable.
7. La Agencia, en su condición de encargado del tratamiento, actuará de conformidad con los siguientes términos y condiciones recogidos en la disposición adicional cuarta de sus Estatutos:

a) Tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público.

b) Garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de

00305160

confidencialidad de naturaleza estatutaria derivada de su condición de empleado público. Garantizará el mismo deber de confidencialidad en caso de que el tratamiento se realice por otros encargados a los que, en su caso, recurra.

c) Tomará todas las medidas necesarias de conformidad con el artículo 32 del Reglamento General de protección de datos.

d) Recurrirá únicamente a otros encargados de tratamiento que ofrezcan las garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con las disposiciones del citado Reglamento, y acrediten el cumplimiento del Esquema Nacional de Seguridad o hayan adoptado medidas que puedan considerarse equivalentes.

e) Asistirá al responsable, teniendo en cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de las personas interesadas.

f) Ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36 del citado Reglamento, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado.

g) Seguirá las instrucciones del responsable en lo relativo a la supresión o conservación de los datos personales una vez finalice la prestación de los servicios de tratamiento, de conformidad con lo dispuesto en el ordenamiento jurídico, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros.

h) Pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de sus obligaciones como encargado, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.

i) Informará inmediatamente al responsable si, en su opinión, una instrucción infringe el citado Reglamento u otras disposiciones en materia de protección de datos y seguridad.

8. La Agencia facilitará asesoramiento técnico especializado a los responsables de tratamiento, como apoyo al cumplimiento de sus obligaciones en relación con la protección de datos desde el diseño y por defecto establecidas en el artículo 25 del Reglamento general de protección de datos, sin perjuicio de las funciones del Delegado de protección de datos que corresponda al responsable del tratamiento.
9. Con carácter general, la Agencia podrá recurrir a otros encargados del tratamiento, de conformidad con los apartados 2 y 4 del artículo 28 del Reglamento general de protección de datos.

Cuando la Agencia recurra a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se impondrán a este otro encargado, mediante contrato u otro acto jurídico establecido con arreglo al Derecho de la Unión o de los Estados miembros, las mismas obligaciones de protección de datos que las establecidas para la Agencia, en particular la prestación de garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con las disposiciones del Reglamento General de Protección de Datos.

Si el subencargado incumple sus obligaciones de protección de datos, la Agencia seguirá siendo plenamente responsable ante el responsable del tratamiento por lo que respecta al cumplimiento de las obligaciones del subencargado.

La Agencia mantendrá permanentemente a disposición de los responsables de tratamiento una relación actualizada de los encargados de tratamiento a los que, en su caso, haya recurrido, con la información relevante en relación con el objeto del encargo.

10. Las responsabilidades operativas de la Agencia en su condición de encargada, recaen en los titulares que ostentan las Subdirecciones y la Secretaría General de la Agencia. Será la persona titular de la Dirección General de Estrategia Digital quien las asuma cuando los tratamientos afecten a más de uno de los titulares anteriores mencionados.

00305160

7. Responsable de Seguridad Interior.

En caso de que se considere necesario por la Consejería a la que la Agencia se adscribe, en virtud del volumen o singularidad de los activos de esta Agencia, la responsabilidad de seguridad interior de la Agencia será ejercida por la persona titular de la Secretaría General. Asimismo, corresponderá a la citada Consejería determinar las condiciones y requisitos mínimos que deben contener el Plan de Seguridad Interior, pudiendo corresponderle en este caso si así se determina las siguientes funciones:

a) Garantizar la seguridad del entorno y sistemas auxiliares de los activos TIC y de la información, tales como vigilancia y control de accesos al edificio, suministro eléctrico, sistemas de detección y contraincendios, refrigeración del centro de proceso de datos y salas técnicas, protección frente a inundaciones y, en general, cualquier amenaza física.

b) Adoptar las medidas de seguridad que le competan dentro de las dispuestas por el Comité de Seguridad Interior, Seguridad TIC y Protección de Datos, informando de su implantación, eficacia e incidentes.

c) El soporte técnico, asesoramiento e información al Comité de Seguridad Interior, Seguridad TIC y Protección de datos, así como la ejecución de sus decisiones y acuerdos en materia de seguridad interior.

d) Proponer las adaptaciones necesarias a su ámbito del modelo general de seguridad interior, incluso valores, tablas y métricas adecuadas al conjunto de los activos en su ámbito.

e) El desarrollo, el mantenimiento y la supervisión del marco regulador de la seguridad interior en la Agencia.

f) La generación y supervisión de criterios y directrices para la gestión de la seguridad interior en el ámbito de la Agencia.

g) La recogida sistemática de información y la supervisión del estado de las principales variables de seguridad interior en el ámbito de la Agencia.

h) El asesoramiento técnico y la auditoría del sistema de seguridad interior en el ámbito de la Agencia.

i) Velar por la coherencia de la aplicación del modelo de seguridad interior en el ámbito de la Agencia, mantenerlo actualizado e impulsar su implantación.

j) Gestionar para el ámbito de la Agencia, la relación con la Unidad de Seguridad Interior de la Consejería.

k) Definir los criterios de protección de activos especialmente sensibles a riesgos que conciernen a la seguridad interior conforme a las especificidades del ámbito de la Agencia.

l) Desarrollar para el ámbito de la Agencia, planes de contingencia en respuesta a incidentes de seguridad interior, incluso situaciones de crisis.

m) Asegurar en el ámbito de la Agencia, el funcionamiento de los mecanismos previstos para recopilar, recibir, analizar y procesar la información relevante para la seguridad interior, destinados a generar inteligencia al respecto.

n) Promover y coordinar la cooperación con las autoridades del sector correspondiente al ámbito material de la Agencia en materia de inteligencia para la seguridad.

ñ) Verificar en su nivel el correcto funcionamiento en la cadena de comunicación y escalado de incidentes de seguridad interior.

o) Elaborar y proponer para aprobación del Comité el Plan de Seguridad Interior de la Agencia.

p) Cuantas otras le sean encomendadas en relación con la seguridad interior por el Comité.

8. Delegado de Protección de Datos.

1. El Delegado de Protección de Datos será designado por la persona titular de la Dirección Gerencia entre empleados públicos, no pudiendo ser removida ni sancionada por desempeñar sus funciones, salvo que incurriera en dolo o

00305160

negligencia grave en su ejercicio. Se garantizará la independencia del Delegado de Protección de Datos dentro de la Agencia, debiendo evitarse cualquier conflicto de intereses.

2. Su designación será comunicada en el plazo de diez días al Consejo de la Transparencia y Protección de Datos de Andalucía.

3. Las funciones y responsabilidades del Delegado de protección de datos son:

a) Poner en conocimiento del Comité las cuestiones relacionadas con la protección de datos que sea necesario y participar, desde el inicio, en todas las cuestiones relacionadas con la protección de datos, contribuyendo así al cumplimiento de la protección de datos personales desde el diseño y por defecto.

b) Asesorar y participar en todo proyecto normativo que pueda afectar al derecho de protección de datos cuando prevea o determine un tratamiento de datos personales y en el proceso de elaboración del análisis del impacto.

c) Ser consultado sobre la contratación, análisis, diseño, operación y mantenimiento de los tratamientos realizados sobre datos personales.

d) Orientar sobre la confección de los modelos de formularios de recogida de datos personales.

e) Asesorar sobre los análisis de riesgos para los derechos y libertades, y sobre la evaluación de impacto relativa a la protección de datos, tanto en la necesidad de su realización como en su elaboración.

f) Supervisar la gestión del registro de actividades de tratamiento de los Responsables de Tratamiento, debiendo éstos facilitarle la información necesaria para ello. Ídem del registro de actividades de tratamiento de la Agencia en su condición de Encargado de tratamiento.

g) Aconsejar al Responsable del Tratamiento sobre la oportunidad y modo de notificar los incidentes de seguridad sobre datos de carácter personal a la autoridad de control correspondiente en materia de protección de datos de carácter personal.

h) Recomendar al Responsable del Tratamiento sobre la oportunidad y modo de informar a las personas interesadas, y a las afectadas por violaciones de la seguridad de sus datos personales que entrañen un alto riesgo para los derechos y libertades de las personas físicas, conforme a lo establecido en el artículo 34 del RGPD.

i) Comprobar la asignación de responsabilidades, la concienciación y formación del personal que participa en las actividades de tratamiento y las auditorías correspondientes.

j) Cooperar con la autoridad de control e intervenir en el caso de reclamaciones. Actuar como punto de contacto de la autoridad de control para cuestiones relativas a los tratamientos, incluidas las consultas previas del artículo 36 del Reglamento, o consultas relativas a cualquier otro asunto.

k) Ser consultado por los interesados para las cuestiones relativas al tratamiento de sus datos personales y el ejercicio de sus derechos.

4. En el ejercicio de sus funciones el Delegado de Protección de Datos tendrá acceso a todos los datos personales y procesos de tratamiento, no pudiendo oponerse a este acceso la existencia de cualquier deber de confidencialidad o secreto. Todos los empleados de la Agencia están obligados a facilitar cuanta información le sea requerida por el Delegado de Protección de Datos, así como el acceso a locales, instalaciones, equipos archivos, soportes de almacenamiento, programas, procesos y procedimientos.

9. Responsables de los Sistemas.

1. Será Responsable del Sistema la persona o personas que dirijan el desarrollo y mantenimiento del sistema de información durante todo su ciclo de vida.

2. Esta responsabilidad recaerá, para cada sistema, en la persona titular del servicio con competencias en el desarrollo y mantenimiento de dicho sistema.

3. Las funciones del Responsable del Sistema serán las siguientes:

a) Gestionar el sistema durante todo su ciclo de vida, desde la especificación de este a la instalación y seguimiento de su funcionamiento.

00305160

b) Velar porque la seguridad TIC esté presente en todas y cada una de las partes del ciclo de vida del sistema contemplando que las directrices de seguridad establecidas de manera horizontal por la Junta de Andalucía se sigan en el desarrollo del sistema.

c) Implementar las medidas de seguridad de los Sistemas de Información y supervisar su correcto funcionamiento en la operación diaria.

d) Verificar de forma previa a su publicación, que existen y están actualizadas las cláusulas y requisitos de seguridad particulares especificados por el Responsable de Seguridad TIC, en los posibles contratos relacionados con el sistema, y posteriormente durante el desarrollo del sistema deberá verificar su cumplimiento. Para ello podrá contar con el asesoramiento de la Unidad de Seguridad TIC Corporativa.

e) Asesorar en la definición de la tipología y política de gestión del sistema, definiendo los criterios de uso y los servicios disponibles en el mismo.

f) Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema.

g) Crear y gestionar la documentación de seguridad del sistema, con el asesoramiento del Responsable de Seguridad TIC.

h) Asesorar, en colaboración con el Responsable de Seguridad TIC, a los Responsables de la Información y a los Responsables de los Servicios en el proceso de análisis y la gestión de riesgos.

i) Investigar los incidentes de seguridad que afecten al sistema, y en su caso, comunicarlos al responsable de seguridad o a quién éste determine. En aquellos que afecten a los derechos y libertades comunicarlo al Responsable o Encargado del tratamiento y al Delegado de protección de datos.

j) Suspender el tratamiento de cierta información o la prestación de un determinado servicio si detecta deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con la persona Responsable de Seguridad TIC y con las personas Responsables del Servicio y de la Información involucradas, antes de ser ejecutada.

Estas tareas se realizarán en colaboración con el resto de las áreas de la Agencia Digital de Andalucía que den soporte al sistema de información, y contarán con el apoyo de dichas áreas para la implantación de las medidas de seguridad.

10. Resolución de conflictos.

1. Los conflictos entre las diferentes personas, unidades u órganos responsables que componen la estructura organizativa de la política de seguridad serán resueltos por el superior jerárquico común. En su defecto, prevalecerá la decisión del Comité.
2. En los conflictos entre las personas responsables que componen la estructura organizativa de la política de seguridad y las personas responsables definidas en la normativa de protección de datos de carácter personal serán resueltos por el Comité, prevaleciendo la decisión que presente un mayor nivel de exigencia respecto a la protección de los datos de carácter personal.

11. Obligaciones de los empleados públicos de la Agencia.

1. Todos los usuarios de los sistemas de información de la Agencia son responsables de la seguridad de los activos tecnológicos puestos a su disposición mediante un uso correcto de los mismos, así como de los datos de carácter personal que manejan.
2. Los empleados públicos que prestan servicios en la Agencia tiene la obligación de conocer y cumplir la política de seguridad y la normativa de seguridad derivada, siendo responsabilidad del Comité disponer los medios necesarios para que la información llegue a las personas afectadas, y que éstas las acepten formalmente.
3. Los nuevos empleados que se incorporen a la Agencia, deberán ser informados de la política de seguridad.

00305160

4. Procederá el ejercicio de las acciones pertinentes, para la exigencia de las responsabilidades legales que correspondan por el incumplimiento manifiesto de la política de seguridad o de la normativa de seguridad derivada.
5. Los empleados públicos deberán cumplir con las instrucciones y normas que regulen las responsabilidades en el uso de los sistemas informáticos y redes de comunicaciones de la Administración de la Junta de Andalucía.
6. Cualquier persona que actúe bajo la autoridad de la persona responsable o de la encargada de un tratamiento de datos personales en el ámbito de aplicación de la Política y tenga acceso a datos personales solo tratará dichos datos siguiendo instrucciones del responsable, salvo que se lo impida el ordenamiento jurídico comunitario, nacional o autonómico.

Cuarto. Gestión de la seguridad.

1. Desarrollo normativo de la seguridad.

1. La presente Política, se desarrollará en distintos niveles con diferente ámbito de aplicación, detalle técnico y obligatoriedad de cumplimiento, pero de manera que cada elemento de desarrollo se fundamente en el nivel superior.
2. Todos estos niveles prestarán especial atención a las exigencias derivadas del Esquema Nacional de Seguridad, así como a la normativa aplicable en materia de protección de datos de carácter personal.
3. La competencia para aprobar las normas o políticas de desarrollo de seguridad de obligado cumplimiento corresponderá en todo caso a la Dirección Gerencia de la Agencia, a propuesta del Comité de Seguridad.
4. Para mayor operatividad la competencia para aprobar procedimientos, instrucciones, directrices, guías o recomendaciones en el ámbito de la seguridad TIC la ostenta la persona titular de la Dirección General de Estrategia Digital. Cuando sean referidas al ámbito de la protección de datos o de la seguridad interior, la competencia la ejerce la persona titular de la Secretaria General. En aquellas materias que exijan la necesaria coordinación de las materias, la competencia para aprobarlos será atribuida a la persona que ostenta la Dirección Gerencia, a propuesta de la Dirección General de Estrategia Digital y de la Secretaria General. En cualquier caso, el Comité de Seguridad de la Agencia deberá ser informado de cualquier procedimiento, instrucción, directriz, guía o recomendación aprobado.
5. El Comité establecerá los mecanismos necesarios para compartir la documentación derivada del desarrollo, con el propósito de regularizarlo o normalizarlo en la medida de lo posible, en todo el ámbito de aplicación de la política de seguridad.

2. Privacidad desde el diseño y por defecto.

1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, la Agencia, en calidad de responsable del tratamiento, aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del Reglamento y proteger los derechos de los interesados.
2. La Agencia, como responsable del tratamiento, aplicará las medidas técnicas y organizativas apropiadas para garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los

00305160

datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

3. En los casos que la Agencia actúa como Encargada, colaborará con los responsables, siempre que sea posible, desde la fase de diseño del tratamiento, advirtiendo sobre posibles riesgos inherentes al mismo y desarrollando sistemas que cumplan con el principio «privacidad desde el diseño y por defecto» recogido en el artículo 25 del RGPD.

3. Gestión de riesgos para la Agencia.

1. La gestión de riesgos para la seguridad interior se acomodará a lo previsto en el Modelo de Seguridad Interior, en el Plan Corporativo de Seguridad Interior, en el Plan de Seguridad Interior de la Consejería a la que se adscribe la Agencia y en los demás instrumentos de planificación previstos en el artículo 17 del Decreto 171/2020, de 13 de octubre.
2. Las personas encargadas de la categorización del nivel de riesgo de los sistemas de información serán los responsables de la Información y de los Servicios, siendo el responsable de Seguridad TIC el encargado de supervisar los análisis de riesgos y proponer las medidas de seguridad a aplicar.
3. El proceso de gestión de riesgos de los sistemas de información, que comprende las fases de categorización de los sistemas, análisis de riesgos y selección de medidas de seguridad a aplicar, que deberán ser proporcionales a los riesgos y estar justificadas, deberá revisarse cuando se produzcan situaciones que cambien el nivel de riesgo (cambios normativos, en la organización, en las tecnologías empleadas, etc.), y al menos con periodicidad anual por parte del responsable de Seguridad TIC y con la colaboración y asesoramiento de la persona delegada de protección de datos, debiendo elevar el primero informe al Comité.
4. La gestión de riesgos de los sistemas de información deberá realizarse de manera continua sobre el sistema de información, conforme a los principios de gestión de la seguridad basada en los riesgos y con reevaluación periódica de los mismos.
5. Cuando un sistema de información trate datos personales le será de aplicación lo dispuesto en el Reglamento General de Protección de Datos y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, el resto de normativa de aplicación, así como los criterios que se establezcan por la Agencia Española de Protección de Datos o en su ámbito competencial, por el Consejo de Transparencia y Protección de Datos de Andalucía, resultándole de aplicación lo que se recoge en el artículo 19 sobre Gestión de riesgos para derechos y libertades de los individuos.
6. En todo caso, prevalecerán las medidas a implantar como consecuencia del análisis de riesgos para los derechos y libertades, en caso de resultar agravadas respecto de las previstas en el Esquema Nacional de Seguridad.
7. Las personas responsables de la Información y de los Servicios y los responsables operativos de los tratamientos cuando los mismos traten datos personales son las responsables de aceptar los riesgos residuales calculados y de realizar su seguimiento y control.

4. Gestión de riesgos para derechos y libertades de los individuos.

1. Los principios fundamentales y los derechos establecidos en el RGPD deberán quedar garantizados por el Responsables del Tratamiento de datos personales con independencia del proceso de gestión de riesgos.
2. Este proceso, en el marco del RGPD, deberá realizarse poniendo el énfasis en las personas y la afectación de sus derechos y libertades como consecuencia del tratamiento de sus datos personales: daños y perjuicios físicos materiales o inmateriales, discriminación, usurpación de identidad o fraude, pérdidas financieras, daños para la reputación, pérdida de confidencialidad de datos sujetos a secreto profesional, reversión no autorizada de la seudonimización de perjuicios

00305160

económicos o sociales, privación a las personas de sus derechos y libertades, que se les impida ejercer el control sobre sus datos personales, y demás riesgos.
Los riesgos para la seguridad de la información deberán ser gestionados, a diferencia de los anteriores, centrados en la protección de los intereses de la Agencia.

3. En consecuencia las medidas técnicas y organizativas de mitigación de los riesgos del RGPD no deberán confundirse con los controles de seguridad de la información establecidos en el ENS.
4. Los responsables operativos del tratamiento en la Agencia han de realizar un análisis de riesgos conforme al artículo 24 del Reglamento General de Protección de Datos.
5. La gestión de los riesgos para los derechos y libertades de las personas interesadas en los tratamientos en los que la Agencia actúa en calidad de encargado del tratamiento se hará en los términos y condiciones que se recogen en el apartado 3 de la disposición adicional cuarta del Decreto 128/2021, de 30 de marzo, por el que se aprueban los Estatutos de la Agencia Digital de Andalucía.
6. En este sentido la Agencia tiene como obligación ayudar al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36 del Reglamento General de Protección de Datos, por tanto, en la gestión del riesgo teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado (artículo 28.3.f).
7. Los responsables y encargados, teniendo en cuenta los elementos enumerados en los artículos 24 y 25 del Reglamento General de Protección de Datos, determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme a la normativa aplicable.
8. En el plan de tratamiento de riesgos, para llevar a cabo la implantación de las medidas, tanto técnicas como organizativas, se identificarán las obligaciones que asume cada parte interviniente en las diferentes fases del ciclo de vida del tratamiento.
9. En los casos que la Agencia actúa como encargada, asumirá la implantación de las medidas que le correspondan según su implicación en el tratamiento, y siempre siguiendo las instrucciones de los responsables.
10. Se establecerán canales ágiles de comunicación entre responsables y Agencia para comunicar brechas de seguridad y para la atención de ejercicio de derechos

5. Evaluaciones de Impacto relativas a la protección de datos Personales.

1. La Evaluación de Impacto en Protección de Datos (EIPD) es una obligación específica del responsable, de conformidad a lo que se establece en el artículo 35.1 del RGPD. Esto supone que es este quien asume las responsabilidades que se derivan de su ejecución y de los resultados que arroje.
2. Los responsables operativos del tratamiento en la Agencia han de realizar una evaluación de impacto en aquellos casos en los que resulte de aplicación.
3. Si la Agencia actúa como encargada, ayudará al cumplimiento de las obligaciones de los responsables de realizar la EIPD en aquellas fases del ciclo de vida del tratamiento en los que la Agencia intervenga. Dicha colaboración por parte de la Agencia tendrá en cuenta la naturaleza del tratamiento y la información a disposición del encargado (art. 28.3.f)., delimitando el alcance de la misma a las fases del ciclo de vida del tratamiento donde ésta intervenga, para que a los responsables les sirva de apoyo en el cumplimiento de sus obligaciones.

6. Auditorías de la seguridad.

1. Los sistemas de información serán objeto de una auditoría regular ordinaria, al menos bianual, que verifique el cumplimiento de los requerimientos del ENS. Estas auditorías ordinarias, así como las extraordinarias, se practicarán de acuerdo con lo establecido en el artículo 31 del Real Decreto 311/2022, de 3 de mayo, y en la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de

00305160

Información, aprobada por Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública.

2. Los informes de auditoría serán presentados por la persona coordinadora de los responsables del Sistema, al Delegado de Protección de Datos, si afectara a éstos, y a la persona responsable de Seguridad TIC. Estos informes serán analizados por esta última persona que presentará sus conclusiones a la persona coordinadora de los responsables del Sistema para que adopte las medidas correctoras adecuadas. Los resultados obtenidos determinarán las líneas de actuación a seguir y las posibles modificaciones a realizar sobre los controles y la normativa de seguridad.
3. Con el fin de optimizar la utilización de los recursos públicos y garantizar una mejor coordinación entre Seguridad TIC y Seguridad de Protección de Datos, siempre que sea posible, las auditorías de seguridad de sistemas de información y las auditorías de protección de datos o medidas análogas de verificación, evaluación y valoración de seguridad de los tratamientos se realizarán de manera conjunta.

7. Clasificación y control de activos.

1. Los recursos informáticos y la información de la Agencia se encontrarán inventariados, con una persona responsable asociada, y en caso de ser necesario, una persona encargada de la custodia de los mismos. Los inventarios se mantendrán actualizados para asegurar su validez.
2. Los activos de información estarán clasificados de acuerdo con su sensibilidad, criticidad y nivel de riesgo para el desarrollo de la actividad de la Agencia en función de la cual se establecerán las medidas de seguridad exigidas para su protección.

8. Formación y concienciación.

Anualmente se desarrollarán actividades de formación y concienciación en seguridad TIC, y en protección de datos destinadas a las personas empleadas públicas de la Agencia. Entre tales actividades se incluirán las de difusión de esta política de seguridad y de su desarrollo normativo.

00305160