1. Disposiciones generales

CONSEJERÍA DE SOSTENIBILIDAD Y MEDIO AMBIENTE

Orden de 13 de marzo de 2025, por la que se establece la política de seguridad de las tecnologías de la información y comunicaciones, seguridad interior, y protección de datos personales de la Consejería de Sostenibilidad y Medio Ambiente.

El Esquema Nacional de Seguridad en el ámbito de la administración electrónica (en adelante, ENS), cuyo objeto es el establecimiento de los principios y requisitos de una política de seguridad en la utilización de medios electrónicos que permita la adecuada protección de la información, actualmente incluido en el artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, se regula por el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Su finalidad última es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a la ciudadanía y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

Para dar cumplimiento a los requisitos y finalidades del ENS en su propio ámbito, la Junta de Andalucía aprobó 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, cuyo artículo 10 ordena que cada Consejería en su ámbito de aplicación disponga formalmente de su propio Documento de Política de Seguridad TIC aprobado por su persona titular.

El citado decreto creó un Comité de Seguridad de las Tecnologías de la Información y Comunicaciones (TIC) corporativo para toda la Junta de Andalucía dependiente de la Consejería competente en materia de dirección e impulso de la política de telecomunicaciones y seguridad de los sistemas de información, junto con un grupo de personas expertas en seguridad TIC de la Administración de la Junta de Andalucía. Además, estableció que cada Consejería y ente instrumental de la Administración de la Junta de Andalucía debían constituir su propio Comité de Seguridad TIC mediante Orden de cada Consejería.

Por otro lado, para la gestión ordinaria de la seguridad disponía la existencia de un Responsable de Seguridad corporativo y uno en cada Consejería o ente instrumental a designar por el respectivo Comité de Seguridad TIC. Esta figura asumiría las funciones de Responsable de Seguridad descritos en la normativa reguladora del Esquema Nacional de Seguridad.

Posteriormente, el Decreto 70/2017, de 6 de junio, modificó el Decreto 1/2011, de 11 de enero. Dicha modificación, según su exposición de motivos, respondía a la necesidad de reforzar el gobierno de la seguridad TIC en la Administración de la Junta de Andalucía y se centraba, fundamentalmente, en introducir cambios en la organización corporativa de la seguridad TIC, potenciando la estructura de gobierno mediante la definición de atribuciones específicas a las Consejerías en relación con su propia seguridad y con la de las entidades vinculadas o dependientes de ellas, clarificando la aplicación del principio de función diferenciada y delimitando las funciones que deben desempeñar las distintas áreas implicadas en el mantenimiento de la seguridad, en línea con los perfiles con responsabilidad en seguridad definidos en la normativa reguladora del Esquema Nacional de Seguridad.

Consecuentemente, la novedad más significativa fue la sustitución del Responsable de Seguridad TIC tanto corporativo como de las Consejerías por una Unidad de Seguridad TIC corporativa de la Junta de Andalucía y en otra Unidad de Seguridad TIC

00317426

por cada Consejería (y también en el Servicio Andaluz de Salud y en el Servicio Andaluz de Empleo) con funciones más definidas, cuya persona titular sería la que asumiría el papel, funciones y responsabilidades encomendados al Responsable de Seguridad por el Esquema Nacional de Seguridad. Solamente los entes instrumentales mantendrían la figura del Responsable de Seguridad TIC como puesto unipersonal y no como unidad.

En cumplimiento del artículo 11 del ENS, sobre el principio de función diferenciada, la responsabilidad de la seguridad de los sistemas de tecnologías de información y comunicaciones estará diferenciada de la responsabilidad sobre la prestación de servicios.

En la elaboración de esta orden se ha tenido en cuenta la normativa actualmente aplicable en materia de datos personales, en especial 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 (Reglamento general de protección de datos); la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y 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.

En la presente orden se adopta una política de protección de datos personales de la Consejería, que se considera proporcionada al importante volumen y nivel de riesgo de los tratamientos de datos que lleva a cabo la Consejería, de conformidad con lo dispuesto en el artículo 24.2 del Reglamento General de Protección de Datos y el artículo 27.2 de la Ley Orgánica 7/2021, de 26 de mayo. En esta política se han recogido medidas que ya se venían adoptando proactivamente, sin ser obligatorias, y que se ha demostrado en la praxis que se trata de buenas prácticas que han mejorado la gestión de la protección de los datos personales en la Consejería.

Con el Decreto 171/2020, de 13 de octubre, se establece la Política de Seguridad Interior en la Administración de la Junta de Andalucía. La organización así resultante tendrá para cada uno de los niveles: corporativo, de Consejería y de provincia; un órgano colegiado identificado como comité con funciones de carácter deliberativo y decisorio, y sendas unidades que darán soporte al sistema y tendrán carácter ejecutivo.

Cerrando el modelo, una persona o equipo, responsables de la seguridad interior para los activos de cada Consejería en cada provincia, serán el verdadero nodo de integración del funcionamiento del sistema.

Teniendo en cuenta los principios de simplificación, economía, eficacia y eficiencia administrativas se ha aconsejado evitar la creación ex-novo de un comité para la seguridad interior en cada Consejería, optando por incluir las que hubieran sido sus funciones y tareas entre las de los actuales Comités de Seguridad TIC, que deberán modificar su denominación, funciones y –eventualmente– composición para incluir los relativos al ámbito de la seguridad interior. Esta solución organizativa supone además un nuevo avance en la coordinación entre la seguridad física y la ciberseguridad, favoreciendo las sinergias posibles entre ambas materias.

En consecuencia, para dar cumplimiento a lo dispuesto en el Decreto 171/2020, de 13 de octubre, se dicta por la Consejería de Agricultura, Pesca y Desarrollo Sostenible, la Orden de 30 de marzo de 2021 por la que se establece la política de seguridad de la información.

El Decreto 170/2024, de 26 de agosto, por el que se establece la estructura orgánica de la Consejería de Sostenibilidad y Medio Ambiente, dispone en su disposición transitoria cuarta que «A los efectos del cumplimiento de lo dispuesto en el artículo 10 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, y en tanto la Consejería no disponga de una Política de Seguridad TIC propia,

00317426

se regirá por la establecida en la Orden de 30 de marzo de 2021, por la que se establece la política de seguridad de la información de la Consejería de Agricultura, Ganadería, Pesca y Desarrollo Sostenible, en lo que le resulte aplicable. Igualmente continuará en funciones el Comité de Seguridad de la Información establecido en aquella y requerido por el citado artículo 10 del Decreto 1/2011, y por el artículo 9 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.

Por tanto, es necesario la aprobación de una orden de la Consejería de Sostenibilidad y Medio Ambiente que establezca la Política de Seguridad de Tecnologías de la Información y Comunicaciones, Seguridad Interior y protección de datos de datos personales.

Por lo expuesto, en la presente orden se abordará por un lado la regulación, composición y régimen de funcionamiento del Comité de Seguridad Interior y Seguridad TIC. Además regulará los objetivos de la política de seguridad interior y de la seguridad TIC y protección de datos personales de la Consejería de Sostenibilidad y Medio Ambiente.

También se ha tenido en cuenta la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) núm. 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2).

Por último, esta orden tiene en cuenta las competencias atribuidas a la Agencia Digital de Andalucía en materia de desarrollo y ejecución de las políticas de seguridad de los sistemas de información y telecomunicaciones, y de gestión de los recursos comunes para la prevención, detección y respuesta a incidentes y amenazas de ciberseguridad en el ámbito de la Administración de la Junta de Andalucía y del sector público andaluz.

La orden consta de cuarenta y siete artículos, distribuidos en cuatro capítulos, una disposición derogatoria y dos disposiciones finales.

El Capítulo I contiene las disposiciones generales sobre el objeto de la presente orden y su ámbito de aplicación. Contiene la regulación del Comité de Seguridad Interior y Seguridad TIC de la Consejería de Sostenibilidad y Medio Ambiente , su composición, atribuciones y régimen de funcionamiento. Dispone la existencia en su seno de un Grupo de Respuesta a Incidentes en los Sistemas de Información para la toma urgente de decisiones en caso de contingencia grave que afecte a la seguridad de los sistemas de información críticos de esta Consejería.

El Capítulo II se refiere a la política de seguridad interior de esta Consejería, regulando la estructura organizativa de la gestión de la seguridad interior en la misma, así como la gestión de riesgos y auditorías de seguridad en esta materia.

El Capítulo III se refiere a la política de seguridad TIC de esta Consejería, regulando así la estructura organizativa de la gestión de seguridad TIC en la misma, así como la gestión de riesgos y auditorías de seguridad en esta materia.

El Capítulo IV está dedicado a aspectos organizativos para recoger la incidencia de la normativa de protección de datos, y especialmente del Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, que aprueba el Reglamento General de Protección de Datos, que afectan directamente a la seguridad TIC. Entre ellos el principio de integridad y confidencialidad de los datos personales recogido en su artículo 5.1.f). que supone que los datos personales serán tratados de tal manera que se garantice una seguridad adecuada de los mismos, 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. Además de asumir la incidencia de los aspectos fundamentales del nuevo Reglamento General de Protección de Datos, recoge sus figuras fundamentales, como son el Responsable del Tratamiento, el Encargado del Tratamiento y el Delegado de Protección de Datos, en la política de seguridad TIC y Seguridad Interior de la Consejería.

00317426

En la elaboración y tramitación de la presente orden, se ha actuado conforme a los principios de buena regulación a los que se refiere el artículo 129.1 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. En cuanto a los principios de necesidad y eficacia, la orden no hace sino desarrollar el artículo 10.1 del Decreto 1/2011, de 11 de enero, como estaba obligada, teniendo el rango normativo de orden en cumplimiento de lo dispuesto en su apartado 2; cumple con el de proporcionalidad al desarrollar estrictamente con el mandato del decreto, no imponiendo más obligaciones a la ciudadanía ni a la Administración que los establecidos en él y regulando figuras necesarias para el cumplimiento de la finalidad perseguida; sobre el de seguridad jurídica, se han tenido en cuenta todas las normas europeas, estatales y autonómicas de aplicación; acerca del de transparencia, al tratarse de una disposición de organización interna no ha habido consulta previa ni trámite de audiencia a la ciudadanía, limitándose los informes a los internos de la Administración; y, por fin, es eficiente porque no sólo evita imponer cargas administrativas adicionales, sino que se limita a utilizar los recursos ya existentes para dar los servicios requeridos sin que suponga ningún incremento de gasto.

En la elaboración de esta orden se ha tenido en cuenta la perspectiva de igualdad de género, de conformidad con la Ley 12/2007, de 26 de noviembre, para la promoción de la igualdad de género en Andalucía y la Ley Orgánica 3/2007, de 22 de marzo, para la igualdad efectiva de mujeres y hombres.

En su virtud, a propuesta de la Secretaría General Técnica de la Consejería, en uso de las atribuciones que me vienen conferidas por el artículo 26 de la Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía, el Decreto del Presidente 169/2024 de 29 de julio, sobre reestructuración de Consejerías, y el Decreto 170/2024, de 26 de agosto, por el que se establece la estructura orgánica de la Consejería de Sostenibilidad y Medio Ambiente,

D I S P O N G O

CAPÍTULO I

Disposiciones generales

Artículo 1. Objeto.

1. En aplicación del Real Decreto 311/2022, de 3 de mayo, la presente orden tiene por objeto establecer la política de seguridad de esta Consejería en los siguientes ámbitos:

a) Seguridad de las tecnologías de la información y comunicaciones (en adelante TIC), en cumplimiento con lo establecido en el artículo 10.2 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, y demás disposiciones que resulten de aplicación.

b) Seguridad interior, en el marco de lo contemplado en el Decreto 171/2020, de 13 de octubre, por el que se establece la Política de Seguridad Interior de la Junta de Andalucía y demás disposiciones que resulten de aplicación.

c) Protección de datos personales, en el marco de lo recogido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos), así como en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y demás disposiciones que resulten de aplicación.

2. La presente orden también tiene por objeto regular la organización funcional de la seguridad TIC y seguridad interior en la Consejería.

00317426

Artículo 2. Ámbito de aplicación.

1. La política de seguridad TIC se aplicará a todos los sistemas de información que son responsabilidad de la Consejería, para el ejercicio de las competencias que tiene atribuidas, siempre que sean utilizados en el ámbito de la Administración de la Junta de Andalucía, por alguno de los órganos o unidades administrativas centrales o periféricos que dependan funcionalmente de la Consejería. Asimismo, deberá ser observada por aquellas personas que tengan acceso a sus sistemas de información.

2. La política de seguridad TIC definida en esta Orden también será de aplicación a todas las entidades vinculadas o dependientes de la Consejería mientras no dispongan de una Política de Seguridad TIC propia.

3. Lo establecido en esta orden en relación con la Política de Seguridad Interior, será de aplicación tanto en la Consejería como en sus entidades vinculadas o dependientes mientras no dispongan de una Política de Seguridad Interior propia.

4. La política de protección de datos personales se aplicará a todas las actividades de tratamiento de responsabilidad de los órganos de la Consejería en el ejercicio de las competencias que tiene atribuidas. También será aplicable a las actividades de tratamiento que los órganos de la Consejería lleven a cabo por cuenta de otros responsables del tratamiento en calidad de encargados, en lo que no se oponga a lo establecido en el acto jurídico de encargo de tratamiento, en las instrucciones o políticas del responsable.

Artículo 3. Comité de Seguridad Interior y Seguridad TIC.

El Comité de Seguridad Interior y Seguridad de las Tecnologías de la Información y Comunicaciones, (en adelante, Comité de Seguridad Interior y Seguridad TIC), actuará como órgano de dirección y seguimiento en materia de seguridad de los activos TIC y del tratamiento de datos personales de titularidad de la Consejería o cuya gestión tenga encomendada. Asimismo, y de acuerdo con lo dispuesto en el artículo 9 del Decreto 171/2020, de 13 de octubre, le corresponderá la dirección y seguimiento en materia de seguridad interior.

Artículo 4. Composición del Comité de Seguridad Interior y Seguridad TIC.

1. El Comité de Seguridad Interior y Seguridad TIC estará compuesto por las siguientes personas:

a) Presidencia: La persona titular de la Viceconsejería.

b) Vicepresidencia: La persona titular de la Secretaría General Técnica.

c) Vocalías: Las personas titulares de todos los órganos directivos centrales y la persona titular de la Coordinación General de la Secretaría General Técnica.

d) Secretaría: La persona titular del Servicio de sistemas de información sectorial asignado a la Consejería, con voz y voto. En los casos de vacante, ausencia, enfermedad u otra causa legal, será sustituida por una persona funcionaria que designe la presidencia del Comité de Seguridad Interior y Seguridad TIC.

e) La persona titular de la Unidad de Seguridad TIC, la de la Unidad de Seguridad Interior y la persona o personas que asuman la figura del Delegado o Delegada de Protección de Datos asistirán en calidad de personas asesoras a las reuniones del Comité, salvo que puntualmente se disponga lo contrario de forma expresa por parte de la presidencia. El Comité podrá convocar a sus reuniones a las personas que en cada caso autorice la presidencia, por propia iniciativa o a propuesta de cualquiera de sus miembros. Así mismo podrá recabar del personal técnico especializado, propio o externo, la información pertinente para la toma de decisiones.

2. En caso de vacante, ausencia, enfermedad u otras causas legales, la persona titular de la Presidencia será sustituida por la persona titular de la Vicepresidencia. Tanto la Vicepresidencia como las Vocalías podrán designar una persona que les sustituya en estas circunstancias entre personal funcionario que ocupe puestos de trabajo de nivel 28 o superior.

00317426

3. 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, 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.

Artículo 5. Funciones del Comité de Seguridad Interior y Seguridad TIC.

1. Al Comité le corresponde aplicar, en el ámbito de la Consejería, las previsiones contenidas en la normativa reguladora del Esquema Nacional de Seguridad en el ámbito de la administración electrónica (en adelante, ENS), y en la normativa reguladora de la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía y determinar la política de seguridad que se ha de emplear en la utilización de los medios electrónicos que permita la adecuada protección de la información.

2. En particular, le corresponde:

a) Aprobar el desarrollo de la política de seguridad TIC de segundo nivel y de Seguridad Interior,

b) Velar por el desarrollo, implantación, concienciación, formación y divulgación, así como por el cumplimiento y actualización de la política de seguridad TIC y Seguridad Interior en la Consejería.

c) Planificar y priorizar las iniciativas necesarias para cumplir con las directrices, los objetivos y los principios básicos marcados en la presente política de seguridad TIC y Seguridad Interior. En especial, la elaboración, actualización y reevaluación periódica de los análisis de riesgos necesarios.

d) Proporcionar, dentro de los límites establecidos en los programas asignados por las leyes anuales de presupuestos a la Consejería, los medios y recursos necesarios para posibilitar la realización de las iniciativas planificadas.

e) Coordinar a alto nivel todas las actuaciones de seguridad, velando para que la definición y el desarrollo de las mismas se adecúen en todo momento a las directrices marcadas por la política de seguridad TIC y Seguridad Interior, involucrando a las diferentes áreas implicadas.

f) Velar para que todos los ámbitos de responsabilidad y actuación en relación a la seguridad TIC y Seguridad Interior, así como su tratamiento queden perfectamente definidos, aprobando los nombramientos necesarios para ello. Especialmente, para asegurar que la totalidad de miembros de la estructura de seguridad definida conozcan sus funciones y responsabilidades.

g) Designar un Grupo de Respuesta a Incidentes de Seguridad de la Información.

h) Designar la persona responsable la Unidad de Seguridad TIC de la Consejería.

i) Designar la persona responsable que ostentará la condición de Responsable de Seguridad Interior de la Consejería.

j) Promover y fomentar la divulgación y formación en cultura de la seguridad TIC y cultura de la Seguridad Interior, así como la mejora continua de la seguridad en la organización, aprobando los planes de mejora de seguridad TIC propuestos por la Unidad de Seguridad TIC, y velando por la asignación y cumplimiento de las responsabilidades oportunas. Así como los planes de mejoras de Seguridad Interior propuestos por la Unidad de Seguridad Interior, y velando por la asignación y cumplimiento de las responsabilidades oportunas.

k) Velar porque la seguridad TIC se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.

l) Coordinar que el desarrollo normativo que tenga incidencia en el desarrollo o explotación de sistemas de información se adecúa a lo establecido en la política de seguridad TIC y Seguridad Interior.

00317426

m) Resolver los conflictos que puedan aparecer entre las diferentes personas responsables o entre diferentes áreas de la organización en materia de seguridad TIC y Seguridad Interior.

n) Coordinar las medidas técnicas y organizativas apropiadas establecidas en la normativa de protección de datos personales, para garantizar un nivel de seguridad adecuado al riesgo, de acuerdo con los correspondientes análisis de riesgos y, en su caso, con las evaluaciones de impacto relativas a la protección de datos, contando con el asesoramiento de la persona o personas que asuman la figura del Delegado o Delegada de Protección de Datos.

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

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

p) El establecimiento de directrices comunes y la supervisión del cumplimento de la normativa de seguridad interior.

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

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

s) Las previsiones para la designación de los Puntos Coordinadores de Seguridad Interior.

Artículo 6. Régimen de funcionamiento del Comité de Seguridad Interior y Seguridad TIC.

1. El Comité de Seguridad Interior y Seguridad TIC 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.

2. El Comité podrá ser convocado, celebrar sus sesiones, adoptar acuerdos y aprobar actas, tanto de forma presencial como utilizando redes de comunicación a distancia, con las medidas adecuadas que garanticen la identidad de las personas comunicante, la confidencialidad y la autenticidad de la información entre ellas transmitida, de conformidad con lo establecido en el artículo 91.3 de la Ley 9/2007, de 22 de octubre. Las personas miembros del Comité están obligadas a respetar la confidencialidad de toda la información a la que tengan acceso.

3. El Comité se regirá por esta orden, 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, así como por el resto de normativa aplicable, como la reguladora del ENS y las normativas de seguridad interior y de protección de datos personales.

Artículo 7. Grupo de Respuesta a Incidentes Críticos en los Sistemas de la Información.

1. El Comité de Seguridad Interior y Seguridad TIC nombrará un Grupo de Respuesta a Incidentes de Seguridad de la Información, cuya función será la toma urgente de decisiones en caso de contingencia grave que afecte a la seguridad de los sistemas de información críticos de la Consejería. Será la persona titular de la Presidencia del Comité quien determine la existencia de tales contingencias y las califique como graves. Las decisiones adoptadas por este grupo serán ratificadas por el Comité en su conjunto cuando sea necesario.

2. La composición del Grupo de Respuesta a Incidentes de Seguridad de la Información vendrá determinada por el Comité contando con el apoyo del Responsable de Seguridad TIC, Responsable de Seguridad Interior y el o la Delegado o Delegada de Protección de Datos de la Consejería. Esta composición podrá variar según requiera el Incidente ocurrido.

3. Corresponde al Grupo de Respuesta a Incidentes de Seguridad de la Información, entre sus funciones, notificar a la autoridad competente en materia de seguridad de las

00317426

redes y sistemas de información, concretamente a su equipo de respuesta a incidentes de seguridad informática (CSIRT o CERT), los incidentes de seguridad TIC, en los casos y en los términos que determine la normativa aplicable.

4. La notificación mencionada en el apartado anterior podrá realizarse bien directamente, bien a través de AndalucíaCERT o por el medio o procedimiento que disponga la política de seguridad de las tecnologías de la información y comunicaciones de la Junta de Andalucía que determine la Dirección General competente en materia de desarrollo y ejecución de las políticas de seguridad de los sistemas de información y telecomunicaciones de la Administración de la Junta de Andalucía y del sector público andaluz o el Comité Corporativo de Seguridad interior de la Junta de Andalucía.

Artículo 8. Obligaciones del personal.

1. Todo el personal que preste servicios en la Consejería tiene la obligación de conocer y cumplir la política de seguridad TIC y Seguridad Interior, la normativa de seguridad derivada y la política de protección de datos personales siendo responsabilidad del Comité de Seguridad Interior y Seguridad TIC disponer los medios necesarios para que la información llegue a las personas afectadas.

2. Todo el personal que se incorpore a la Consejería o vaya a tener acceso a alguno de sus sistemas de información o la información gestionada por ellos deberá ser informado de la política de seguridad TIC y Seguridad Interior.

3. 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 TIC, Seguridad Interior o de la normativa de seguridad derivada, y en materia de protección de datos personales.

4. El personal de la Consejería deberá cumplir además con las instrucciones y normas que regulen el comportamiento del personal empleado público en el uso de los sistemas informáticos y redes de comunicaciones de la Administración de la Junta de Andalucía.

5. Cualquier persona que actúe bajo la autoridad del responsable o del encargado de un tratamiento de datos personales en el ámbito de aplicación de esta orden y tenga acceso a datos personales solo tratará dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del ordenamiento jurídico de la Unión Europea o del Estado español.

6. Todo el personal que preste servicios en la Consejería está comprometido con la preservación de la seguridad interior, siendo responsable de utilizar correctamente los activos y de participar, durante el desempeño ordinario de sus funciones y tareas, en la detección precoz de cuantos indicios puedan servir a la prevención de riesgos para la seguridad interior.

Artículo 9. Resolución de conflictos.

1. Los conflictos entre las diferentes personas, unidades u órganos responsables que componen la estructura organizativa de la Política de Seguridad Interior serán resueltos por el superior jerárquico común. En su defecto, prevalecerá la decisión del Comité de Seguridad Interior y Seguridad TIC.

2. Los conflictos entre las diferentes personas, unidades u órganos responsables que componen la estructura organizativa de la Política de Seguridad TIC serán resueltos por el superior jerárquico común. En su defecto, prevalecerá la decisión del Comité de Seguridad Interior y Seguridad TIC.

3. En los conflictos entre las personas responsables que componen la estructura organizativa de la Política de Seguridad Interior, Política de Seguridad TIC y la Política de Protección de Datos Personales, prevalecerá la decisión que presente un mayor nivel de exigencia respecto a la protección de los datos personales. En cualquier caso, cuando la persona o personas que asuman la figura del Delegado o Delegada de Protección de Datos aprecien la existencia de una vulneración relevante en materia de protección de

00317426

datos lo documentará y lo comunicará inmediatamente al órgano directivo que tenga la condición de responsable o al encargado del tratamiento.

4. En todos los apartados anteriores les será aplicable el artículo 110 de la Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía.

CAPÍTULO II

Política de seguridad interior

Artículo 10. Objetivos en materia de seguridad interior.

1. La política de seguridad interior contra riesgos intencionales persigue la consecución de los siguientes objetivos:

a) Asegurar el funcionamiento como sistema eficaz, eficiente y explícitamente definido, de toda la actividad que la Consejería despliegue para la prevención de daños intencionales sobre su personal y personas usuarias, sobre sus activos y sobre la continuidad de su funcionamiento y servicios, así como para la reacción cuando tales daños se produzcan.

b) Garantizar el cumplimiento de toda la normativa que sea de aplicación a las actuaciones de la Consejería en esta materia.

c) Colaborar a la seguridad a través de la protección del personal, personas usuarias y activos de la Consejería.

2. La preservación de la seguridad interior será considerada objetivo común de todas las personas al servicio de la Consejería, siendo éstas responsables de utilizar correctamente los activos y de participar, durante el desempeño ordinario de sus funciones y tareas, en la detección precoz de cuantos indicios puedan servir a la prevención de riesgos para la seguridad interior.

Artículo 11. Principios básicos en materia de seguridad interior.

La política de seguridad interior de la Administración de la Junta de Andalucía se desarrollará, con carácter general, de acuerdo con los siguientes principios:

a) Anticipación y prevención.

b) Eficiencia y sostenibilidad en el uso de los medios.

c) Preservación de la resiliencia.

d) Unidad de acción, coordinación y colaboración.

e) Prioridad en la protección de la vida y salud de las personas frente a la integridad de los activos.

f) Proporcionalidad en los costes económicos y operativos de las medidas de seguridad.

g) Mantenimiento de la integridad, disponibilidad y continuidad en el funcionamiento de los activos.

h) Aseguramiento de la continuidad de los servicios.

i) Responsabilidad estratificada, identificable y compartida.

j) Actuación planificada.

Artículo 12. Unidad de Seguridad Interior.

La Consejería, de acuerdo con lo establecido en el artículo 10 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, contará con una Unidad de Seguridad Interior que desempeñará las funciones relacionadas en el citado artículo y que tendrá como responsables a las personas designadas por el Comité de Seguridad Interior y Seguridad TIC.

Artículo 13. Organización y gestión de la seguridad interior.

La estructura organizativa de la gestión de la seguridad interior en la Consejería está compuesta por las siguientes figuras:

00317426

a) El Comité de Seguridad Interior y seguridad de las Tecnologías de la Información y Comunicaciones.
b) La Unidad de Seguridad Interior.
c) Los puntos coordinadores de seguridad interior en cada provincia.

Artículo 14. Responsable de Seguridad Interior.
La persona responsable de la Unidad de Seguridad Interior de la Consejería tendrá la condición de Responsable de Seguridad Interior, en los términos que establece el Decreto 171/2020, de 13 de octubre.

Artículo 15. Gestión de los riesgos en materia de seguridad interior.
La gestión de los 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 y en los demás instrumentos de planificación previstos en el artículo 17 del Decreto 171/2020, de 13 de octubre.

Artículo 16. Auditorías de la seguridad en materia de seguridad interior.
Las auditorías realizadas en la Consejería en materia de seguridad interior se realizarán conforme a las previsiones que se contengan en el Modelo de Seguridad Interior, en el Plan Corporativo de Seguridad Interior, en el Plan de Seguridad Interior de la Consejería y en los demás instrumentos de planificación previstos en el artículo 17 del Decreto 171/2020, de 13 de octubre.

Artículo 17. Clasificación y control de activos en materia de seguridad interior.
En relación con la Seguridad Interior, la clasificación y control de activos 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 de Sostenibilidad y Medio Ambiente y en los demás instrumentos de planificación previstos en el artículo 17 del Decreto 171/2020, de 13 de octubre.

CAPÍTULO III

Política de seguridad TIC

Artículo 18. Objetivos en materia de seguridad TIC.
Son objetivos de la política de seguridad TIC:
a) Garantizar la seguridad TIC y proteger los activos o recursos de información.
b) Definir la estructura de la organización de la seguridad TIC de la Consejería.
c) Marcar las directrices, los objetivos y los principios básicos de seguridad TIC de la Consejería.
d) Orientar la organización para la prestación de servicios basados en la gestión de riesgos.
e) Servir de marco de desarrollo de las normas, procedimientos y procesos de gestión de la seguridad TIC.

Artículo 19. Desarrollo de la seguridad TIC en la Consejería.
1. Las medidas sobre la seguridad TIC, de obligado cumplimiento, se desarrollarán en cuatro 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. Dichas medidas conformarán el Plan Director de Seguridad de los Sistemas de Información de la Consejería.
2. En todos estos niveles se prestará especial atención a las exigencias derivadas del Esquema Nacional de Seguridad, así como a la normativa aplicable en materia de protección de datos personales.

00317426

3. Los niveles de desarrollo son los siguientes:

a) Primer nivel: Política de seguridad TIC, constituido por la presente Orden. Es de obligado cumplimiento en toda la Consejería.

b) Segundo nivel: Normas de seguridad. Son de obligado cumplimiento en toda la Consejería y deben ser aprobadas por el Comité de Seguridad Interior y Seguridad TIC. Describen de forma general los principios y normas de seguridad que serán concretados en los niveles posteriores.

c) Tercer nivel: Procedimientos. Describen las acciones a realizar, de una manera más específica, en un proceso relacionado con la seguridad. Son dependientes de las normas de seguridad y serán aprobados por la persona titular de la Secretaría General Técnica.

d) Cuarto nivel: Documentación técnica. En este último nivel se puede incluir todo tipo de documentación técnica o especializada que se considere necesario para completar y facilitar el desarrollo de las medidas de seguridad. La aprueba la persona titular del Servicio de sistemas de información sectorial asignado a la Consejería.

4. El Comité de Seguridad Interior y Seguridad TIC establecerá los mecanismos necesarios para compartir la documentación derivada del desarrollo con el propósito de regularizarlo, en la medida de lo posible, en todo el ámbito de aplicación de la política de seguridad TIC.

La siguiente tabla resume el marco de desarrollo y la competencia para su aprobación:

Nivel	Documento	Aprueba
Primero	Política de seguridad	Persona titular de la Consejería de Sostenibilidad y Medio Ambiente.
Segundo	Normas de seguridad	Comité de Seguridad Interior y Seguridad TIC
Tercero	Procedimientos	Persona titular de la Secretaría General Técnica
Cuarto	Documentación técnica	Titular del Servicio de sistemas de información sectorial de la Agencia Digital de Andalucía asignado a la Consejería o bien titular de la unidad administrativa correspondiente

5. La Unidad de Seguridad TIC se encargará de la gestión de los documentos indicados, debiendo asegurar que ésta sea completa y proporcione información suficiente para definir las necesidades de protección de la información y los activos asociados a la misma en el ámbito de la Consejería.

Artículo 20. Principios básicos en materia de seguridad TIC.

Los principios básicos que regirán la política de seguridad TIC de la Consejería serán, además de los establecidos en la normativa reguladora de la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía y en el ENS, en el ámbito de la administración electrónica, los siguientes:

a) Principio de prevención. Se evitará, o al menos prevendrá en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello, se deben implementar las medidas mínimas de seguridad determinadas por las normas y leyes que le sean de aplicación, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, estarán claramente definidos y documentados.

b) Principio de detección. Dado que los servicios se pueden degradar rápidamente debido a incidentes que, en función de su gravedad, pueden producir desde una simple desaceleración hasta la detención de los mismos, se debe monitorizar la operación de los servicios de manera continua para detectar anomalías en los niveles de prestación requeridos, actuando en consecuencia. La monitorización es especialmente relevante para establecer líneas de defensa. Para ello, se implantarán mecanismos de detección, análisis y reporte que lleguen a las personas responsables regularmente, a efectos de

00317426

detectar cuándo se produce una desviación significativa de los parámetros de servicio marcados.

c) Principio de reacción. Deberá minimizarse el tiempo requerido de recuperación, de forma que el impacto de los incidentes de seguridad sea el menor posible, para lo cual se establecerán mecanismos para responder eficazmente a los incidentes de seguridad, designando un punto de contacto para centralizar y gestionar el intercambio de información asociada a los incidentes de seguridad, así como estableciendo protocolos para el intercambio de información relacionada con dichos incidentes.

d) Principio de recuperación: Se deberá garantizar, en la medida de lo posible, la disponibilidad de los servicios ofrecidos a la ciudadanía, en función de la criticidad de los mismos.

e) Principio de vigilancia continua: En todo momento, se deberá de realizar una vigilancia continua que permita la detección de actividades o comportamientos anómalos que habiliten a la Consejería a proporcionar una repuesta oportuna. Esta vigilancia continua, al mismo tiempo, permitirá realizar una evaluación permanente del estado de la seguridad de los activos que forman parte de la Consejería, facilitando la medición de la evolución, detección de vulnerabilidades e identificación de las deficiencias de configuración que corresponda al activo de información. Esta evaluación de la seguridad por cada activo, permite a la Consejería reevaluar y actualizar de forma permanente las medidas de seguridad de sus activos, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección.

f) Disponibilidad, Integridad y confidencialidad de los datos personales: Los datos personales serán tratados de tal manera que se garantice un nivel de seguridad adecuado al riesgo para los derechos y libertades de las personas físicas, 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.

Artículo 21. Unidad de Seguridad TIC.

1. La Consejería, de acuerdo con lo establecido en el artículo 11 del Decreto 1/2011, de 11 de enero, contará con una Unidad de Seguridad TIC, garantizando el principio de función diferenciada recogido en el artículo 5.j) de dicho decreto, y contemplado en el artículo 11 del ENS, que ejerza las funciones de Responsabilidad de Seguridad TIC de la Consejería, debiendo ser designada la persona responsable de la citada Unidad entre personal funcionario por el Comité de Seguridad TIC de la misma.

2. La Unidad de Seguridad TIC tendrá las siguientes atribuciones, de acuerdo con lo dispuesto en el artículo 11.1. del Decreto 1/2011, de 11 de enero:

a) Labores de soporte, asesoramiento e información al Comité de Seguridad TIC de la Consejería, así como de ejecución de las decisiones y acuerdos adoptados por éste.

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

c) Definición, implantación y mantenimiento de los controles de carácter organizativo para la protección de los datos, aplicaciones y sistemas, así como la gestión de riesgos en materia de seguridad TIC de la Consejería.

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

e) Definición 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 Consejería por parte de los Servicios o Departamentos 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 de evolutivos de los existentes, la Unidad de Seguridad TIC deberá evaluar los aspectos de seguridad y comunicar los posibles riesgos al Responsable de la Información y Responsable del Servicio.

00317426

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

g) Coordinación, dirección y seguimiento de la actividad en materia de seguridad TIC de las entidades vinculadas o dependientes de la Consejería, en el momento en que se apruebe la política de seguridad TIC de dichas entidades.

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

i) Y cuantas otras le sean encomendadas por el órgano directivo de la Consejería del que dependa funcional u orgánicamente.

Artículo 22. Organización y gestión de la seguridad TIC.

1. La estructura organizativa de la gestión de la seguridad TIC de la Consejería, en relación con el ENS en el ámbito de la administración electrónica, está compuesta por las siguientes figuras:

a) El Comité de Seguridad Interior y seguridad TIC.

b) El Grupo de Respuesta a Incidentes en los Sistemas de Información.

c) Unidad de Seguridad TIC, la persona responsable de esta Unidad de Seguridad tendrá la condición de Responsable de Seguridad TIC en dicha Consejería.

d) Responsables de la Información.

e) Responsables del Sistema.

f) Responsables del Servicio.

2. Además, en el ámbito de la Consejería, las siguientes figuras ostentan atribuciones directamente relacionadas con la seguridad TIC, que son las que les asigna la normativa sobre protección de datos personales:

a) Responsables de los tratamientos de datos personales.

b) Encargados de los tratamientos de datos de datos personales.

c) El Delegado o Delegada de Protección de Datos, en adelante DPD.

Artículo 23. Responsable de Seguridad TIC.

La persona responsable de la Unidad de Seguridad TIC de la Consejería tendrá la condición de Responsable de Seguridad TIC, en los términos establecidos en la normativa reguladora del Esquema Nacional de Seguridad.

Artículo 24. Responsable de la Información.

1. Los Responsables de la Información serán los órganos directivos que determinarán los requisitos de la información tratada.

2. Las principales funciones, dentro de su ámbito de actuación, son las siguientes:

a) Ayudar a determinar los requisitos de seguridad TIC, categorizando la información mediante la valoración de los impactos de los incidentes que puedan producirse.

b) Proporcionar la información necesaria a la Unidad de Seguridad TIC para realizar los preceptivos análisis de riesgos, con la finalidad de establecer las salvaguardas a implantar. Para ello contará con la ayuda de los Responsables de los Servicios y 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 los mismos.

Artículo 25. Responsable del Servicio.

1. Los Responsables de los Servicios serán las personas titulares de los órganos directivos o unidades administrativas que determinarán los requisitos de los servicios prestados.

2. Las principales funciones, dentro de su ámbito de actuación, son las siguientes:

00317426

a) Determinar los requisitos de seguridad de los servicios a prestar, categorizando los servicios mediante la valoración de los impactos de los incidentes que puedan producirse.

b) Proporcionar la información necesaria a la Unidad de Seguridad TIC para realizar los preceptivos análisis de riesgos, con la finalidad de establecer las salvaguardas a implantar. Para ello contará con la ayuda de los Responsables de la Información y de los 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 los mismos.

Artículo 26. Responsable del Sistema.

1. El Responsable del Sistema será la persona que, por sí o a través de recursos propios o contratados, se encargará de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad. Además, figurarán en la documentación de seguridad de los sistemas de información. Para cada sistema de información deberá existir una persona Responsable de Sistema, siendo posible que una misma persona sea responsable de varios sistemas.

2. Las responsabilidades en materia de Seguridad TIC que ostentará el Responsable del Sistema serán:

a) Supervisar el desarrollo, operación y mantenimiento de los sistemas de información durante todo su ciclo de vida, así como las especificaciones de los mismos, la instalación y verificación de su correcto funcionamiento.

b) Ser la primera persona responsable de la seguridad de los sistemas de información que dirija, velando porque la seguridad TIC esté presente en todas y cada una de las partes de sus ciclos de vida. Especialmente deberá velar por que el desarrollo de los sistemas siga las directrices de seguridad establecidas de manera horizontal por la Junta de Andalucía de acuerdo con los criterios y requisitos técnicos de seguridad aplicables definidos por la Unidad de Seguridad TIC de la Consejería.

c) Creación, mantenimiento y actualización continua de la documentación de seguridad de los sistemas de información, con el asesoramiento de la Unidad de Seguridad TIC.

d) Asesorar en la definición de la topología y sistema de gestión de los sistemas de información estableciendo los criterios de uso y los servicios disponibles en el mismo.

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

f) Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.

g) Asesorar en colaboración con la Unidad de Seguridad TIC, a los Responsables de la Información y a los Responsables de los Servicios, en el proceso de la gestión de riesgos en materia de seguridad TIC.

h) Suspender el manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con las personas Responsables de la Información afectada, del Servicio afectado y con la Unidad de Seguridad TIC, antes de ser ejecutada.

Artículo 27. Los Puntos o Personas de Contacto (POC).

De conformidad con lo previsto en el apartado 5, del artículo 13 del ENS, en el caso de servicios externalizados, salvo por causa justificada y documentada, la organización prestataria de dichos servicios deberá designar un POC (Punto o Persona de Contacto) para la seguridad de la información tratada y el servicio prestado, que cuente con el apoyo de los órganos directivos, y que canalice y supervise, tanto el cumplimiento de los requisitos de seguridad del servicio que presta o solución que provea, como las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes

00317426

para el ámbito de dicho servicio. Dicho POC de seguridad será el propio Responsable de Seguridad de la organización contratada, formará parte de su área o tendrá comunicación directa con la misma.

Artículo 28. Función diferenciada.

De conformidad con lo previsto en apartado 3, del artículo 13 del ENS, el Responsable de Seguridad TIC será distinto del Responsable del Sistema, no debiendo existir dependencia jerárquica entre ambos. En aquellas situaciones excepcionales en las que la ausencia justificada de recursos haga necesario que ambas funciones recaigan en la misma persona o en distintas personas entre las que exista relación jerárquica, deberán aplicarse medidas compensatorias para garantizar la finalidad del principio de diferenciación de responsabilidades previsto en el artículo 11 del ENS.

Artículo 29. Clasificación y control de activos en materia de Seguridad TIC.

1. Los recursos informáticos y la información de la Consejería se encontrarán inventariados, con una persona responsable asociada y, en caso de ser necesario, una persona custodia de los mismos. Los inventarios se mantendrán actualizados para asegurar su validez.

2. Los activos de información estarán clasificados de acuerdo a su sensibilidad y criticidad para el desarrollo de la actividad de la Consejería, en función de la cual se establecerán las medidas de seguridad exigidas para su protección.

Artículo 30. Gestión de riesgos en materia de Seguridad TIC.

1. La gestión de riesgos 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.

2. En cumplimiento de lo previsto en el artículo 41 del ENS, la facultad para efectuar las valoraciones a las que se refiere el artículo 40 del ENS, así como, en su caso, su posterior modificación, corresponderá al responsable o responsables de la información o servicios afectados. Con base en las valoraciones señaladas, la determinación de la categoría de seguridad del sistema corresponderá al responsable o responsables de la seguridad.

3. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos personales, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, así como la comunicación o acceso no autorizados a dichos datos.

4. El Responsable del Servicio o el Responsable de la Información será el encargado de aceptar los riesgos residuales calculados en el análisis sobre la información y los servicios, y de realizar su seguimiento y control.

5. El proceso de gestión de riesgos, 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 al menos con periodicidad anual por parte de la Unidad de Seguridad TIC, que elevará un informe al Comité de Seguridad TIC.

Artículo 31. Auditorías de la seguridad en materia de Seguridad TIC.

1. Los sistemas de información serán objeto de una auditoría regular ordinaria, cada dos años, que verifique el cumplimiento de los requerimientos del ENS. Estas auditorías ordinarias, así como las extraordinarias se harán de acuerdo con lo establecido en el artículo 31 del ENS.

2. Los informes de auditoría serán presentados a la persona responsable del sistema competente, al Delegado o Delegada de Protección de Datos, si afectara a estos, y a la

00317426

persona responsable de la Unidad de Seguridad TIC. Estos informes serán analizados por esta última persona que presentará sus conclusiones a la persona Responsable 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.

CAPÍTULO IV

Política de protección de datos personales

Artículo 32. Objetivos de la política de protección de datos personales.

1. La presente orden tiene como objetivo establecer las directrices generales de actuación y funcionamiento en materia de protección de datos personales en la Consejería, al objeto de garantizar el cumplimiento de lo dispuesto en el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016; la Ley Orgánica 3/2018, de 5 de diciembre; 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, y demás normativa que resulte de aplicación.

2. La presente política de protección de datos personales de la Consejería se adopta como medida de responsabilidad proactiva demostrable, proporcionada al importante volumen y nivel de riesgo de los tratamientos de datos que lleva a cabo la Consejería, de conformidad con lo dispuesto en el artículo 24.2 del Reglamento General de Protección de Datos y el artículo 27.2 de la Ley Orgánica 7/2021, de 26 de mayo.

Artículo 33. Principios básicos en materia de protección de datos personales.

De conformidad con lo dispuesto en el artículo 5 del Reglamento General de Protección de Datos, los datos personales serán tratados con arreglo a los principios de:

a) Licitud, lealtad, transparencia.
b) Limitación de la finalidad.
c) Minimización de los datos.
d) Exactitud.
e) Limitación del plazo de conservación.
f) Integridad y confidencialidad.
g) Responsabilidad proactiva.

Artículo 34. Adopción, ámbito de aplicación y marco normativo.

1. Se adopta la política de protección de datos personales de la Consejería como medida de responsabilidad proactiva demostrable, proporcionada al importante volumen y nivel de riesgo de los tratamientos de datos que lleva a cabo la Consejería, de conformidad con lo dispuesto en el artículo 5,2 y 24.2 del Reglamento General de Protección de Datos, el artículo 27.2 de la Ley Orgánica 7/2021, de 26 de mayo, y Capítulo I del Titulo V de la Ley Orgánica 3/2018 Ley de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

2. Esta política de protección de datos personales de la Consejería será de aplicación a todas las actividades de tratamiento de responsabilidad de los órganos de la Consejería en el ejercicio de las competencias que tiene atribuidas. También será aplicable a las actividades de tratamiento que los órganos de la Consejería lleven a cabo por cuenta de

00317426

otros responsables del tratamiento en calidad de encargados, en lo que no se oponga a lo establecido en el acto jurídico de encargo de tratamiento o en las instrucciones o políticas del responsable.

3. Esta política de protección de datos personales de la Consejería se aplicará en el marco de lo dispuesto en 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 Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016 y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

4. En dicho ámbito, cada Responsable del Tratamiento de datos personales aplicará las medidas técnicas y organizativas apropiadas a fin de garantizar y ser capaz de demostrar que los tratamientos de datos personales son conformes con dicha normativa, de acuerdo con el principio de responsabilidad proactiva, según lo previsto en el artículo 5.2 del Reglamento General de Protección de Datos y el artículo 6.5 de la Ley Orgánica 7/2021, de 26 de mayo.

Artículo 35. Responsables de los tratamientos de datos personales.

1. Los Responsables de los tratamientos de datos personales son los órganos de la Consejería respecto a los tratamientos sobre los que determinen sus fines y medios, salvo que las normas aplicables sobre asignación de atribuciones en materia de protección de datos personales dispongan otra cosa.

2 .La condición de Responsable del tratamiento coincidirá con la de Responsable de la Información.

Artículo 36. Encargados de los tratamientos de datos personales.

1. En el caso en el que los Responsables de los tratamientos designaran a un Encargado del tratamiento, lo harán únicamente a uno que ofrezca garantías suficientes para aplicar las medidas técnicas y organizativas apropiadas para que el tratamiento sea conforme al Reglamento General de Protección de Datos y garantice la protección de los derechos de las personas interesadas, de conformidad con el artículo 28 del Reglamento General de Protección de Datos. Dicho encargado tratará los datos exclusivamente por cuenta del responsable, siguiendo las instrucciones documentadas de este, a no ser que esté obligado a ello en virtud del ordenamiento jurídico de la Unión Europea o del Estado español.

2. El tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión Europea o de los Estados miembros de la misma, incluido el ordenamiento jurídico español, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable y las estipulaciones previstas en el artículo 28.3 del Reglamento General de Protección de Datos y demás normativa de aplicación.

3. Dichas estipulaciones se incluirán, al menos, en los siguientes actos jurídicos:

a) Todos los contratos, incluidos los menores.

b) Encargos a medios propios.

c) Encomiendas de gestión.

d) Convenios que impliquen encargo de tratamiento de datos.

e) Subvenciones que impliquen encargo de tratamiento de datos.

4. Su incorporación se efectuará de acuerdo con los modelos tipo de pliegos recomendados por la Comisión Consultiva de Contratación Pública y con los modelos de documentos propios de la Consejería que se harán públicos en la intranet y la red social corporativa y con las instrucciones en materia de contratación y otras materias.

00317426

5. Cuando se requiera de la Agencia Digital de Andalucía la realización de actuaciones que supongan un encargo de tratamiento de datos personales, éste se regirá por las estipulaciones como encargada del tratamiento de la Administración de la Junta de Andalucía que constan en sus Estatutos. Estas estipulaciones se completarán con un documento emitido en el momento de la toma de requisitos donde se especificarán:

a) Las actividades de tratamiento afectadas que sean responsabilidad de órganos de la Consejería.

b) Las categorías de datos.

c) Las categorías de personas interesadas.

d) El nivel de seguridad mínimo exigido, por protección de datos personales, en cada una de las dimensiones de la seguridad, de conformidad con el Esquema Nacional de Seguridad.

e) El alcance geográfico y temporal del tratamiento.

Artículo 37. Delegado o Delegada de Protección de Datos.

1. La Consejería contará con una persona o grupo de personas que ostenten la condición de Delegado o Delegada de Protección de Datos a efectos de lo establecido en los artículos 37 a 39 del Reglamento General de Protección de Datos y, cuando sea de aplicación, en los artículos 40 a 42 de la Ley Orgánica 7/2021, de 26 de mayo. Su ámbito de actuación se extenderá a los órganos de la Consejería. No obstante, su ámbito de actuación se podrá extender a entidades instrumentales adscritas a la Consejería a las que se considere aconsejable, por su reducido tamaño o reducido volumen o nivel de riesgo de los tratamientos de datos personales que lleven a cabo. En el caso de órganos periféricos, su ámbito de actuación se limitará a las actividades de tratamiento que lleven a cabo en el ejercicio de las competencias propias de esta Consejería.

2. La figura del Delegado o Delegada de Protección de Datos podrá ser asumida por una persona o grupo de personas de la Consejería, bien en base a la existencia de una o más plazas específicas en la Relación de Puestos de Trabajo o bien por simple asignación de funciones, de acuerdo con la legislación vigente. La persona o personas que asuman la figura del Delegado o Delegada de Protección de Datos serán designadas por la persona titular de la Viceconsejería entre personal funcionario adscrito a la Consejería, gozando de independencia funcional, sin que puedan recibir instrucciones sobre el desempeño de sus funciones, ni ser removidas o sancionadas por dicho desempeño, salvo que incurriera en dolo o negligencia grave.

En el caso de que la figura del DPD la asuma un grupo de personas, se designará a una de ellas como representante del grupo.

El personal funcionario que asuma la figura del Delegado o Delegada de Protección de Datos deberá contar con conocimientos especializados en derecho y la práctica en materia de protección de datos, sistemas de información y seguridad de la misma, procesos, servicios y estructura de la entidad y normativa aplicable a la entidad y procedimientos administrativos, garantizándose los recursos suficientes para desarrollar su labor de forma efectiva, y comunicándose al Consejo de Transparencia y Protección de Datos de Andalucía, en el plazo de diez días, su designación, nombramiento y cese, conforme al artículo 34.3 de la LOPDGDD.

3. Son funciones de la persona o personas que asuman la figura del Delegado o Delegada de Protección de Datos, además de la supervisión del cumplimiento de la política de protección de datos personales de la Consejería, las establecidas en los artículos 35.2 y 39.1 del RGPD, en los artículos 36.1, 37 y 65.4 de la LOPDGDD, y, en su caso, en el artículo 42 de la Ley Orgánica 7/2021, de 26 de mayo, que son las siguientes:

a) Informar y asesorar al responsable o al encargado del tratamiento y al personal que se ocupen del tratamiento de las obligaciones que les incumben en materia de protección de datos personales.

00317426

b) Supervisar el cumplimiento de lo dispuesto en la normativa sobre protección de datos personales y en la política de protección de datos personales de la Consejería, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.

c) Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos, tanto en la necesidad de su realización como en su elaboración y en la necesidad o no de consulta previa a la autoridad de control, y supervisar su aplicación.

d) Actuar como punto de contacto entre la Consejería y el Consejo de Transparencia y Protección de Datos de Andalucía, en cuanto autoridad de control en materia de protección de datos, para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36 del Reglamento General de Protección de Datos, y realizar las otras consultas que se puedan suscitar en la materia.

Artículo 38. Registro de actividades de tratamiento.

1. Cada órgano responsable del tratamiento llevará un registro de las actividades de tratamiento de datos personales efectuadas bajo su responsabilidad, de acuerdo con lo establecido en el artículo 30 del Reglamento General de Protección de Datos y el resto de normativa de datos personales aplicable.

2. Cada órgano encargado del tratamiento llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable, de acuerdo con el precepto citado en el apartado anterior. Cuando un mismo órgano ostente la condición de responsable de unas actividades de tratamiento y de encargado de otras, podrá incluir en un mismo registro dichas actividades de tratamiento de datos personales, siempre que quede definido con claridad cuales efectúa como responsable y cuales como encargado por cuenta de otro responsable .

3. La persona titular del órgano aprobará mediante resolución la creación, actualización y modificación del registro de las actividades de tratamiento de datos personales de dicho órgano comunicándolo a la persona o personas que asuman la figura del Delegado o Delegada de Protección de Datos.

4. Los registros de las actividades de tratamiento de datos personales de los órganos de la Consejería, una vez aprobados, se publicarán junto con su base legal en el Inventario de Actividades de Tratamiento de la Administración de la Junta de Andalucía en su portal web, de conformidad con el artículo 6 bis de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

5. Al objeto de ofrecer una mayor claridad y transparencia hacia la ciudadanía, las actividades de tratamiento de igual contenido en todas las Delegaciones Territoriales de Sostenibilidad y Medio Ambiente en cada provincia, se registrarán de manera uniforme y se publicarán conjuntamente en el Inventario de Actividades de Tratamiento de la Administración de la Junta de Andalucía. El resto de las actividades de tratamiento que sean específicas de alguna Delegación Territorial concreta se registrarán y publicarán separadamente.

Artículo 39. Ejercicio de derechos en materia de protección de datos personales.

1. Una Instrucción de la Viceconsejería establecerá un protocolo para la atención del ejercicio de derechos de las personas interesadas en materia de protección de datos personales.

2. Dicho protocolo recogerá tanto las obligaciones impuestas a la Consejería por la normativa de protección de datos personales como las impuestas por cualquier otra normativa aplicable a las administraciones públicas, como la de procedimiento administrativo común o la de documentación y archivos.

3. Las solicitudes de ejercicio de derechos serán resueltas mediante resolución de la persona titular del órgano responsable del tratamiento, y en dicha resolución se

00317426

dispondrán las medidas técnicas y organizativas que fueran pertinentes para satisfacer el derecho a la protección de datos personales de las personas interesadas. No obstante, se podrán adoptar cautelarmente dichas medidas técnicas y organizativas a la mayor brevedad y antes de que recaiga resolución con el fin de evitar o minimizar los posibles perjuicios a los derechos y libertades de las personas interesadas.

Artículo 40. Protección de datos personales desde el diseño y por defecto.

1. Conforme al principio de protección de datos personales desde el diseño, al que se refiere el artículo 25.1 del Reglamento General de Protección de Datos, el 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, a fin de cumplir los requisitos de dicho Reglamento y proteger los derechos de las personas interesadas.

2. Conforme al principio de protección de datos personales por defecto del artículo 25.1 del Reglamento General de Protección de Datos, el responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a 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 datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

3. Se garantizará ambos principios desde el diseño en la elaboración de cualquier proyecto, plan, disposición de carácter general, contrato, acto jurídico que se vaya a aprobar o sistema de información que se vaya a desarrollar o contratar.

4. Para garantizar la aplicación de los principios de protección de datos desde el diseño y por defecto en el procedimiento de elaboración de disposiciones generales, el órgano directivo proponente incorporará, en la documentación previa al acuerdo de inicio, una memoria de garantía del principio de protección de datos personales desde el diseño y por defecto suscrita por su titular. Esta memoria será puesta en conocimiento de la persona que ostente la condición de Delegado o Delegada de Protección de Datos por parte de la unidad administrativa u órgano que lleve a cabo la tramitación del procedimiento, y contendrá, al menos, referencia a:

a) Si la aprobación del proyecto requeriría un alta, baja o modificación de actividades de tratamiento en el Registro de Actividades de Tratamiento. En caso de alta o modificación se incluiría, además, la información establecida en el artículo 30 del RGPD y su base legal.

b) Si se han aplicado los principios de protección de datos por defecto y de minimización.

c) Si la aprobación del proyecto conllevará la puesta en funcionamiento o modificación de algún tipo de tratamiento que requiera la realización de una Evaluación de Impacto relativa a la Protección de Datos personales.

d) Si la aprobación del proyecto conlleva algún encargo de tratamiento o comunicación de datos personales.

e) Si el tratamiento contempla la existencia de decisiones automatizadas individuales, incluida la elaboración de perfiles y, en su caso, las medidas adecuadas para salvaguardar los derechos, libertades e intereses legítimos de las personas interesadas.

5. La persona titular del órgano responsable de la tramitación del procedimiento en la Consejería solicitará a la Comisión Consultiva de la Transparencia y la Protección de Datos el preceptivo informe de los anteproyectos de leyes y proyectos de disposiciones generales elaborados por la Consejería. A tal fin, consultará a la persona o personas que

00317426

asuman la figura del Delegado de Protección de Datos si un determinado anteproyecto de ley o proyecto de disposiciones generales pudiera incidir en dicha materia de protección de datos, de forma que resultase necesaria la emisión del referido informe.

6. Para garantizar la aplicación de los principios de protección de datos desde el diseño y por defecto en los sistemas de información y proyectos TIC, se realizará una valoración de los proyectos desde el punto de vista de protección de datos en la toma de requisitos, y en todo caso con carácter previo a la contratación de los servicios necesarios. La normativa de desarrollo informático y de seguridad TIC incorporará las medidas necesarias para garantizar esta valoración y, de ser necesaria, la participación de la persona que ostente la condición de Delegado o Delegada de Protección de Datos, en la fase de diseño del proyecto, antes de adquirirse compromisos contractuales y económicos.

Artículo 41. Seguridad.

1. Teniendo en cuenta el estado de la técnica, los costes de aplicación y la naturaleza, el alcance, el contexto y los fines del tratamiento de datos personales, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, y de conformidad con el artículo 32 del Reglamento General de Protección de Datos, el Responsable y el Encargado del Tratamiento en el ámbito de aplicación de esta orden, aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) La seudonimización y el cifrado de datos personales.

b) La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

c) La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.

d) Un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. La seguridad de los tratamientos por medios total o parcialmente automatizados se preservará mediante la aplicación del Esquema Nacional de Seguridad, actualmente regulado en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, de conformidad con la disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre. En todo caso, prevalecerán las medidas a implantar como consecuencia del análisis de riesgos y, en su caso, de la evaluación de impacto relativa a la protección de datos, cuando resulten agravadas respecto de las previstas en el Esquema Nacional de Seguridad.

Artículo 42. Seguridad de tratamientos no automatizados.

1. La seguridad de los tratamientos por medios no automatizados y la parte no automatizada de los parcialmente automatizados, como los efectuados en soporte papel, se llevará a cabo a través de la aplicación de la normativa aplicable en materia de protección de datos y de documentación y archivos.

2. Se aplicarán las medidas de seguridad previstas en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos personales en lo que no se oponga a la actual normativa de protección de datos. Consecuentemente, la categorización de los niveles de seguridad aplicables a cada tratamiento no se determinará exclusivamente según las categorías de datos sino en función un análisis de riesgos por protección de datos para los derechos y libertades de las personas interesadas.

3. Los órganos o unidades administrativas competentes en materia de régimen general y asuntos generales, de intendencia y de archivo serán responsables de proporcionar los medios necesarios para la aplicación de dichas medidas, y de adoptar las medidas que sean de general aplicación a la Consejería o, en su caso, a la respectiva Delegación Territorial.

00317426

Artículo 43. Análisis de riesgo por protección de datos personales.

1. Al objeto de determinar las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con la normativa de protección de datos, el responsable realizará, con el asesoramiento de la persona o personas que asuman la figura de Delegado o Delegada de Protección de Datos, por cada actividad de tratamiento de datos, un análisis de riesgo para los derechos y libertades de las personas interesadas, atendiendo a la naturaleza, al ámbito, al contexto y a los fines de la actividad de tratamiento. En la realización del análisis de riesgo deberá seguirse el protocolo aprobado en el artículo 47.1.c) de esta orden.

2. El resultado de los análisis de riesgo se concretará en un documento suscrito por la persona titular del órgano responsable del tratamiento o de la unidad administrativa competente, que incluirá, al menos, los siguientes elementos:

a) Descripción del tratamiento.

b) Riesgos para los derechos y libertades de las personas interesadas.

c) Categorización de los niveles de seguridad y de cada una de las dimensiones de la seguridad de conformidad con el Esquema Nacional de Seguridad.

d) Medidas técnicas y organizativas a adoptar para reducir el riesgo.

e) Aceptación del riesgo residual.

Artículo 44. Evaluación de Impacto relativa a la Protección de Datos (EIPD).

1. Cuando un tipo de tratamiento de datos personal, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el Responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales (EIPD), debiendo seguirse el protocolo al que se refiere el artículo 47.1.c) de esta orden ,de conformidad con el artículo 35 del Reglamento General de Protección de Datos y el resto de normativa aplicable. Para ello recabará el asesoramiento de la persona que ostente la condición de Delegado o Delegada de Protección de Datos.

2. El resultado de la EIPD se concretará en un informe suscrito por la persona titular del órgano responsable del tratamiento que incluirá, al menos:

a) Una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento.

b) Una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad.

c) Una evaluación de los riesgos para los derechos y libertades de las personas interesadas.

d) Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales y para demostrar la conformidad con la normativa en materia de protección de datos personales.

e) La decisión sobre formular o no la consulta previa al Consejo de Transparencia y Protección de Datos de Andalucía a la que se refiere el artículo 36 del Reglamento General de Protección de Datos y demás normativa de aplicación.

3. La consulta previa al Consejo de Transparencia y Protección de Datos de Andalucía a la que se refiere el artículo 36 del Reglamento General de Protección de Datos será suscrita por la persona titular del órgano responsable del tratamiento. La persona que ostente la condición de Delegado o Delegada de Protección de Datos dará traslado de la misma a la autoridad de control.

Artículo 45. Violaciones de la seguridad de datos personales.

1. Se aprobará, mediante instrucción de la Viceconsejería, un protocolo de gestión de posibles violaciones de la seguridad de datos personales, de conformidad con los artículos 33 y 34 del Reglamento General de Protección de Datos y el resto de normativa de datos

00317426

personales aplicable. Mediante este protocolo, que tendrá un carácter complementario respecto al procedimiento de gestión de incidentes de seguridad TIC, se garantizará:

a) La prontitud en la detección de las violaciones, puesta en marcha de las medidas previstas en el protocolo y en la puesta de conocimiento de las personas que deben intervenir en su gestión.

b) La adopción de las medidas de contención, gestión y corrección de las mismas.

c) La notificación de las mismas, en los casos preceptivos, al Consejo de Transparencia y Protección de Datos de Andalucía, como autoridad de control en materia de protección de datos para las entidades públicas andaluzas y la comunicación a las personas interesadas de ser conveniente o legalmente obligatorio.

d) El cumplimiento la obligación legal de documentar todas las violaciones de la seguridad, documentación que estará a disposición de la autoridad de control.

e) La llevanza, por parte de los órganos responsables del tratamiento, de un inventario de violaciones de la seguridad que permita conocerlas y analizarlas, al objeto de disponer de la información necesaria para aplicar un ciclo de mejora continua de la seguridad.

2. En caso de violación de la seguridad de los datos personales, el órgano responsable del tratamiento la notificará a la autoridad de control competente sin dilación indebida y en un plazo máximo de 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.

3. 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 órgano responsable del tratamiento la comunicará a las personas interesadas sin dilación indebida. La comunicación deberá contener como mínimo la información a que se refiere el artículo 34.2 del del Reglamento General de Protección de Datos y podrá omitirse en los casos previstos en el artículo 34.3 del citado Reglamento General.

Artículo 46. Formación, concienciación y sensibilización.

1. El órgano competente en materia de formación del personal de la Consejería, con el asesoramiento de la persona o personas que asuman la figura del Delegado o Delegada de Protección de Datos, elaborará y aprobará un plan anual de formación, concienciación y sensibilización sobre protección de datos personales. Dicho plan será complementario a los planes anuales de formación del resto de entidades que ofrece formación al personal de la Consejería como el Instituto Andaluz de Administración Pública.

Artículo 47. Protocolos e Instrucciones.

1. Se establecerán, mediante Instrucción de la Viceconsejería, protocolos para garantizar un cumplimiento sistemático, uniforme y demostrable de las principales obligaciones en materia de protección de datos personales. En particular, se aprobarán, al menos, los siguientes protocolos:

a) Protocolo sobre atención al ejercicio de derechos en materia de protección de datos, con el contenido previsto en el artículo 39.2 de esta orden.

b) Protocolo sobre gestión de violaciones de la seguridad de datos personales, que contendrá las garantías expresadas en el artículo 45.1 de esta orden.

c) Protocolo sobre gestión de la seguridad de los datos personales, análisis de riesgo por protección de datos personales y evaluación de impacto relativa a protección de datos.

2. Aquellas Instrucciones que versen sobre otros aspectos de la actividad administrativa, tales como contratación, elaboración de disposiciones generales, transparencia u otras, deberán incorporar cualquier aspecto que sea necesario o aconsejable desde el punto de vista de la normativa en materia de protección de datos.

Artículo 48. Comunicaciones oficiales con la autoridad de control.

1. La persona titular del órgano responsable del tratamiento suscribirá los siguientes documentos y comunicaciones relacionados con las potestades del Consejo de

00317426

Transparencia y Protección de Datos de Andalucía como autoridad de control en materia de protección de datos:

a) Aquellos relacionados con reclamaciones y denuncias de las personas interesadas ante la autoridad de control en materia de protección de datos contra la actuación del órgano responsable del tratamiento del que sean titulares.

b) Aquellos relacionados con actuaciones inspectoras de la autoridad de control.

c) Las notificaciones de violaciones de la seguridad de los datos personales a la autoridad de control, de conformidad con el artículo 33 del Reglamento General de Protección de Datos o, en su caso, del artículo 38 de la Ley Orgánica 7/2021, de 26 de mayo.

d) La consulta previa antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de los datos muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para mitigarlo, de conformidad con el artículo 36 del Reglamento General de Protección de Datos o, en su caso, en el artículo 36 de la Ley Orgánica 7/2021, de 26 de mayo.

e) Las consultas generales sobre cumplimiento de obligaciones e interpretación de la normativa en materia de protección de datos.

f) Los demás documentos relacionados con la autoridad de control que sean de competencia del órgano responsable del tratamiento.

2. La persona que ostente la condición de Delegado o Delegada de Protección de Datos, en su condición de interlocutor con la autoridad de control, dará traslado a los órganos responsables del tratamiento de las comunicaciones y documentos que le sean remitidos desde la autoridad de control. Así mismo, dará traslado a la autoridad de control de las comunicaciones y documentos mencionados en el apartado anterior a ella dirigidos que reciba de los órganos responsables del tratamiento, sin perjuicio de que estos los remitan directamente a dicha autoridad de control o por ausencia o indisponibilidad de la persona que ostente la condición de Delegado o Delegada de Protección de Datos.

Artículo 49. Auditorías internas y externas e Inspección General de Servicios.

1. El órgano competente para la coordinación de las tareas necesarias para el cumplimiento de la legislación vigente en materia de protección de datos elaborará y aprobará un plan bienal de auditoría en la Consejería. La persona o personas que asuman la figura del Delegado o Delegada de Protección de Datos prestarán su asesoramiento en la elaboración de dicho plan.

2. El plan de auditoría incluirá acciones anuales de auditoría interna sectorial, centrados en aspectos concretos o sectores de actividad de la Consejería. Se emitirá un informe anual con los resultados de las auditorías realizadas que se pondrá en conocimiento de los órganos responsables del tratamiento afectados, del Comité de Seguridad Interior y TIC y de la persona o personas que asuman la figura del Delegado o Delegada de Protección de Datos.

3. En el segundo año del plan se llevará a cabo una auditoría externa, ya sea general o centrada en los aspectos concretos que se establezcan en el plan. Los resultados de las auditorías externas se pondrán en conocimiento de los órganos responsables del tratamiento afectados y del Comité de Seguridad Interior y TIC.

4. Los informes de resultados de las acciones inspectoras realizadas por la Inspección General de Servicios se pondrán en conocimiento de los órganos responsables del tratamiento afectados y del Comité de Seguridad Interior y TIC.

Disposición derogatoria única. Derogación normativa.

Quedan derogadas cuantas disposiciones de igual o inferior rango que se opongan a lo dispuesto en esta orden.

00317426

Disposición final primera. Desarrollo y ejecución.

Se faculta a la persona titular de la Viceconsejería para dictar cuantas instrucciones sean necesarias y adoptar cuantas medidas técnicas sean oportunas para el desarrollo, difusión y ejecución de la presente orden.

Disposición final segunda. Entrada en vigor.

La presente orden entrará en vigor a partir del día siguiente al de su publicación en el Boletín Oficial de la Junta de Andalucía.

Sevilla, 13 de marzo de 2025

CATALINA MONTSERRAT GARCÍA CARRASCO
Consejera de Sostenibilidad y Medio Ambiente

00317426