1. Disposiciones generales

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

Orden de 23 de octubre de 2024, por la que se establece la Política de Seguridad TIC, Seguridad Interior y Protección de Datos Personales de la Consejería de la Presidencia, Interior, Diálogo Social y Simplificación Administrativa.

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, establece en su artículo 1.2 que 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.

Conforme establece el artículo 156.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada.

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.

En su artículo 12, exige que cada Administración Pública cuente con una política de seguridad formalmente aprobada por el órgano competente, la cual deberá establecerse de acuerdo con los principios básicos señalados en el Capítulo II de dicho Real Decreto.

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. Conforme a lo dispuesto en su artículo 1.1, este decreto tiene por objeto definir y regular la política de seguridad de las tecnologías de la información y comunicaciones de la Administración de la Junta de Andalucía, conformando, junto a las disposiciones y documentos técnicos que la desarrollen, el marco regulador de seguridad TIC. Asimismo, su artículo 10.1 establece que cada Consejería y entidad incluida en su ámbito de aplicación deberá disponer formalmente de su propio documento de política de seguridad TIC aprobado por su persona titular.

El citado decreto conforme a lo dispuesto en su artículo 7, crea en el seno de la Comisión Interdepartamental de la Sociedad de la Información de la Junta de Andalucía, como órgano colegiado de coordinación y gobierno en materia de seguridad en el ámbito de la Administración de la Junta de Andalucía, el Comité de Seguridad TIC de la Junta de Andalucía. De otro lado, en su artículo 10.1 dispone que cada Consejería y entidad deberá contar con un Comité de Seguridad TIC, que no tendrá carácter colegiado y que actuará como órgano de dirección y seguimiento en materia de seguridad de los activos TIC de su titularidad o cuya gestión tenga encomendada.

Lo dispuesto en el Decreto 1/2011, de 11 de enero, hizo necesario un cambio en la organización corporativa de la seguridad de la información, creando nuevas estructuras y perfiles con responsabilidad en la seguridad. Por tanto, ante la necesidad de establecer la estructura organizativa recogida en el mismo que da respuesta a las obligaciones impuestas por el Esquema Nacional de Seguridad, se dictó la Orden de la Consejería de la Presidencia, Administración Local y Memoria Democrática, de 30 de agosto de 2018, por la que se establece la política de la seguridad de las tecnologías de la información

00309996

y telecomunicaciones, así como el marco organizativo y tecnológico en el ámbito de la Consejería. Entre otros aspectos a través de la misma, se procedió a crear el Comité de Seguridad TIC de la Consejería.

Por otro lado, en un escenario general en el que los riesgos de daños intencionales se multiplican, se hacía inaplazable abordar como objetivo la explícita definición de un sistema de seguridad interior de la Administración de la Junta de Andalucía para la prevención y reacción ante daños en las personas, el patrimonio y el funcionamiento, intencionadamente provocados por agentes externos, personal propio o usuarios.

En este contexto con fecha 16 de octubre de 2020 entró en vigor 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. El objeto de este decreto, según lo establecido en su artículo 1.1, es establecer una política de seguridad interior en la Administración de la Junta de Andalucía que defina un completo sistema para la prevención y reacción ante daños intencionadamente provocados por agentes externos, personal propio o personas usuarias, contra sus propias personas usuarias, su personal, sus activos y la continuidad de su funcionamiento y servicios.

De otro lado, su artículo 6.1.b) señala que la organización funcional de la seguridad interior en el ámbito de cada Consejería y entidades dependientes debe tener una estructura mínima constituida por un Comité de Seguridad Interior y Seguridad TIC y una Unidad de Seguridad Interior.

Asimismo, el artículo 9 de este decreto determina que las respectivas normas de creación de los Comités de Seguridad TIC a los que alude el artículo 10 del Decreto 1/2011, de 11 de enero, deben modificar su denominación, añadiendo su definición como órganos de dirección y seguimiento en materia de seguridad interior, y actualizando la composición y régimen de los mismos, con descripción incluso de las nuevas funciones a incorporar. Y el artículo 10.1 dispone que cada Consejería y aquellas de sus entidades dependientes en las que estas lo consideren necesario por virtud del volumen o singularidad de los activos, contará con una Unidad de Seguridad Interior.

En el ámbito provincial, serán los servicios periféricos de la Consejería los encargados de gestionar dicha materia, al amparo de lo dispuesto en los artículos 11, 12 y 13 de dicho decreto.

De acuerdo con el preámbulo del Decreto 171/2020, de 13 de octubre, se establece un modelo organizativo mínimo en materia de seguridad interior, «cuyas funciones deberán ser asignadas a elementos preexistentes de las estructuras orgánicas y que por lo tanto no presupone el incremento de otras nuevas, ni de nuevos puestos de trabajo». Con fundamento en los principios de simplificación, economía, eficacia y eficiencia administrativas, el citado decreto ha optado por evitar la creación ex-novo de un Comité para la seguridad interior en cada Consejería o entidad, incluyendo las que hubieran sido sus funciones y tareas entre las de los Comités de Seguridad TIC, que de este modo deberán modificar su denominación, funciones y composición para incluir los aspectos correspondientes al ámbito de la seguridad interior.

En consecuencia, para dar cumplimiento a lo dispuesto en el Decreto 171/2020, de 13 de octubre, se dicta por la Consejería de la Presidencia, Administración Pública e Interior, la Orden de 2 de junio de 2021, por la que se modifica la Orden de 30 de agosto de 2018.

La entrada en vigor del Real Decreto 311/2022, de 3 de mayo, hace necesario la modificación de la Orden de 30 de agosto de 2018, resultando así preferible en aras de seguridad jurídica, la aprobación de una nueva disposición.

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

00309996

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. 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).

En esta orden se adopta una política de protección de datos personales de la Consejería de la Presidencia, Interior, Diálogo Social y Simplificación Administrativa, que se considera proporcionada al importante volumen y nivel de riesgo de los tratamientos de datos que lleva a cabo la misma, 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.

Por su parte, la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, en su artículo 13.h) entre los derechos de las personas en sus relaciones con las Administraciones Públicas, hace referencia al derecho a la protección de los datos personales y, en particular, a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.

Asimismo, la Ley 40/2015, de 1 de octubre, en su artículo 3.2 establece que las Administraciones Públicas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculadas o dependientes a través de medios electrónicos, que aseguren la interoperabilidad y seguridad de los sistemas y soluciones adoptadas, garantizarán la protección de los datos personales y facilitarán preferentemente la prestación conjunta de servicios a las personas interesadas.

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, conforme al artículo 6.3.ñ) y u) de sus estatutos.

Esta orden consta de cincuenta artículos, distribuidos en cuatro capítulos, una disposición derogatoria y tres disposiciones finales.

El Capítulo I contiene las disposiciones generales sobre el objeto de la presente orden y su ámbito de aplicación, así como los objetivos y principios en materia de seguridad TIC y seguridad interior. Contiene la regulación del Comité de Seguridad Interior y Seguridad TIC de la Consejería de la Presidencia, Interior, Diálogo Social y Simplificación Administrativa, 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.

Asimismo, se regulan las auditorías de seguridad en los distintos ámbitos aludidos en la presente orden.

El Capítulo II 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 III 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.

00309996

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 afecta 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 Reglamento General de Protección de Datos, recoge sus figuras fundamentales, como son la de Responsable del Tratamiento, Encargado del Tratamiento y Delegado de Protección de Datos, en la política de seguridad TIC y seguridad interior de la Consejería.

En la elaboración de esta orden se ha tomado en consideración la perspectiva de igualdad de género, de conformidad con el artículo 5 de 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.

También se ha considerado en la elaboración y tramitación de la presente orden, la adecuación de la misma a los principios de buena regulación a los que se refiere el artículo 129.1 de la Ley 39/2015, de 1 de octubre, así como el artículo 7 bis del Decreto 622/2019, de 27 de diciembre, de administración electrónica, simplificación de procedimientos y racionalización organizativa de la Junta de Andalucía. En cuanto al cumplimiento de los principios de necesidad y eficacia, esta orden tiene por finalidad regular los aspectos, tanto organizativos como procedimentales necesarios para la definición de la política de seguridad de la Consejería de la Presidencia, Interior, Diálogo Social y Simplificación Administrativa a los efectos de cumplir con las obligaciones que le son propias en materia de seguridad. Es proporcional y eficiente ya que evita la duplicidad de órganos, no impone ningún tipo de medidas restrictivas de derechos u obligaciones y evita imponer cargas administrativas adicionales por su carácter organizativo e interno, limitándose a utilizar los recursos ya existentes para dar los servicios requeridos sin que suponga ningún incremento de gasto. En cuanto al principio de seguridad jurídica y a la justificación sobre el rango del proyecto normativo y su debida coherencia con el resto del ordenamiento jurídico, se resalta que la competencia para la aprobación de esta norma corresponde a la persona titular de la Consejería, al estar ante el ejercicio de la potestad reglamentaria prevista en el artículo 44.2 de la Ley 6/2006, de 24 de octubre, del Gobierno de la Comunidad Autónoma de Andalucía, y su forma, de conformidad con lo dispuesto en el artículo 46.4 del mismo cuerpo legal, debe ser la de orden. Asimismo, se han tenido en cuenta todas las normas europeas, estatales y autonómicas de aplicación.

Acerca del principio de transparencia, al tratarse de una disposición de organización interna que no afecta directamente a los derechos e intereses legítimos de la ciudadanía, se ha prescindido de los trámites de consulta, audiencia e información pública en virtud de lo dispuesto en el artículo 45.1.f) de la Ley 6/2006, de 24 de octubre.

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 44.2 de la Ley 6/2006, de 24 de octubre, por el artículo 26.2.ª de la Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía, así como en virtud del 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,

00309996

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.

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 todo el personal destinado en dichos órganos y unidades administrativas, así como por aquellas personas que tengan acceso a sus sistemas de información.

2. De acuerdo con lo establecido en el artículo 10 del Decreto 1/2011, de 11 de enero, las entidades vinculadas o dependientes incluidas en el ámbito de aplicación de esta orden deberán disponer formalmente de su propio documento de Política de Seguridad TIC, así como de las disposiciones de desarrollo que adecúen, en su caso, las directrices comunes de la Administración de la Junta de Andalucía a sus particularidades, debiendo ser aprobado por la persona titular de cada entidad.

Sin perjuicio de lo anterior, 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 en coherencia con la presente orden.

3. Lo regulado en la presente orden en relación con la seguridad interior será de aplicación tanto a la Consejería como a sus entidades vinculadas o dependientes.

4. La Política de Protección de Datos Personales se aplicará a todas las actividades de tratamiento responsabilidad de los órganos centrales y periféricos 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 centrales y periféricos 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.

00309996

Artículo 3. Objetivos en materia de Seguridad TIC.

De conformidad con lo establecido en los artículos 4 y 5 del Decreto 1/2011, de 11 de enero, y con los requisitos mínimos previstos en el Real Decreto 311/2022, de 3 de mayo, 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 4. Objetivos en materia de Seguridad Interior.

1. Conforme a lo establecido en el artículo 4 del Decreto 171/2020, de 13 de octubre, 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 estas 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.

3. La seguridad interior implica a todas las áreas de la Consejería, al desplegarse 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.

Artículo 5. Objetivos en materia 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 6. 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

00309996

de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía y en el Esquema Nacional de Seguridad (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, 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 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 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.

Artículo 7. 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.

00309996

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 8. 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 9. 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 10. 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, la persona titular de la Coordinación General de la Secretaría General Técnica y la persona titular de la Coordinación de los Servicios Territoriales y Entidades Adscritas.

d) Secretaría: La persona titular del Servicio con competencias en sistemas de información sectoriales de la Agencia Digital de Andalucía 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) Asesores: El Comité de Seguridad Interior y Seguridad TIC de la Consejería podrá convocar a sus reuniones como asesores a la persona titular de la Unidad de Seguridad TIC, la de la Unidad de Seguridad Interior y la persona que ostente la condición de Delegado de Protección de Datos, así como a otras personas que en cada caso autorice la Presidencia, por propia iniciativa o a propuesta de alguno de sus miembros. Asimismo, 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.

00309996

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, de 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.

Artículo 11. Funciones del Comité de Seguridad Interior y Seguridad TIC.

Serán funciones propias del Comité de Seguridad Interior y Seguridad TIC, como órgano de dirección y seguimiento en materia de seguridad de los activos TIC y del tratamiento de datos personales, así como en materia de seguridad interior en la Consejería:

a) Aprobar el desarrollo de la Política de Seguridad TIC de segundo nivel, de Seguridad Interior y de Protección de Datos Personales.

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, Seguridad Interior y Protección de Datos Personales. En especial, la elaboración, actualización y reevaluación periódica de los análisis de riesgos necesarios.

d) Velar dentro de los límites establecidos en los programas asignados por las leyes anuales de presupuestos a la Consejería, porque sean proporcionados los medios y recursos necesarios para posibilitar la realización de las iniciativas planificadas y de los planes estratégicos definidos.

e) Coordinar a alto nivel todas las actuaciones de seguridad, velando para que la definición y el desarrollo de las mismas se adecuen 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 interior y seguridad TIC, 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 de 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 adecua a lo establecido en la Política de Seguridad TIC, Seguridad Interior y Protección de Datos Personales.

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.

00309996

n) Coordinar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad, de acuerdo con los correspondientes análisis de riesgos para los derechos y libertades de las personas físicas y, en su caso, las evaluaciones de impacto relativas a la protección de datos, contando con el asesoramiento de la persona que ostente la condición de Delegado de Protección de Datos.

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

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.

t) Designar, a propuesta de las personas titulares de las Delegaciones del Gobierno, a los Puntos Coordinadores de Seguridad Interior.

Artículo 12. 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 por semestre y con carácter extraordinario por acuerdo de la Presidencia, a iniciativa propia o previa solicitud razonada de uno de sus miembros. Asimismo, también podrá reunirse cuando se requiera la ratificación en conjunto de la calificación como grave de las contingencias que pudieran afectar a la seguridad de los sistemas de información críticos de la Consejería de la Presidencia, Interior, Diálogo Social y Simplificación Administrativa.

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 comunicantes, así como la integridad, confidencialidad y la autenticidad de la información entre ellas transmitidas, de conformidad con lo establecido en el artículo 91.3 de la Ley 9/2007, de 22 de octubre. Las personas miembros del Comité de Seguridad Interior y Seguridad TIC están obligadas a respetar la confidencialidad de toda 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 13. Grupo de Respuesta a Incidentes de Seguridad 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 de Seguridad Interior y Seguridad TIC quien determine la existencia de tales contingencias y las califique como graves a propuesta del Grupo de Respuestas a Incidentes de Seguridad de la Información. Las decisiones adoptadas por este grupo serán ratificadas por el Comité de Seguridad Interior y Seguridad TIC 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 de Seguridad Interior y Seguridad TIC contando con el apoyo de la persona Responsable de Seguridad TIC, la persona Responsable de Seguridad Interior y la persona que ostente la condición de Delegado de Protección de Datos. 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

00309996

redes y sistemas de información, concretamente a su equipo de respuesta a incidentes de seguridad informática (SOC Andalucía), 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 se realizará 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 el órgano 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 de Seguridad TIC corporativo de la Junta de Andalucía.

Artículo 14. 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, la Política de Seguridad Interior y la Política de Protección de Datos Personales, así como las normativas de seguridad derivadas, 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, la Política de Seguridad Interior y la Política de Protección de Datos Personales.

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 y Seguridad Interior o de la normativa de seguridad derivada, así como por incumplimiento 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, de conformidad con lo establecido en la 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.

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.

5. Todo el personal que preste servicios en la Consejería deberá estar 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 15. 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 y Seguridad TIC serán resueltos por el superior jerárquico común. En su defecto, prevalecerá la decisión del Comité de Seguridad Interior y Seguridad TIC.

2. 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.

Artículo 16. Auditorías de seguridad.

00309996

1. Al menos cada dos años, o con carácter específico y extraordinario cuando se lleven a cabo modificaciones sustanciales que repercutan en el cumplimiento de las medidas implantadas, o ante la existencia de elementos que puedan evidenciar la posible manifestación de un riesgo no evaluado o no previsto, o cuando se estime necesario por el Comité de Seguridad Interior y Seguridad TIC, se realizarán auditorías de seguridad a fin de verificar el cumplimiento de los requerimientos de los marcos normativos aplicables.

Estas auditorías se llevarán a cabo de conformidad con lo establecido en las normas de los diferentes ámbitos de seguridad aludidos en la presente orden.

El alcance de las auditorías deberá incluir la adopción de las medidas técnicas y organizativas que se apliquen para garantizar la seguridad que se requiera para cada caso.

En relación con los sistemas de información de categoría básica, esta auditoría podrá ser sustituida por una autoevaluación en los términos establecidos en el Esquema Nacional de Seguridad.

2. La Unidad de Seguridad Interior, la Unidad de Seguridad TIC y la persona que ostente la condición de Delegado de Protección de Datos, supervisarán las auditorías y emitirán las recomendaciones que estimen oportunas en sus respectivos ámbitos de actuación.

Los informes de auditoría, bajo el conocimiento y supervisión del Comité de Seguridad, serán presentados ante los responsables de las unidades aludidas en el párrafo anterior, así como ante la persona que ostente la condición de Delegado de Protección de Datos, para la valoración de las medidas correctoras propuestas en sus respectivos ámbitos de competencias. Estos, en el plazo de diez días, presentarán sus conclusiones y propuestas para que este Comité apruebe las medidas correctoras adecuadas. Los resultados obtenidos determinarán las líneas de actuación a seguir y las posibles modificaciones a realizar sobre los controles y normas de seguridad.

3. Con el fin de optimizar la utilización de los recursos públicos y garantizar una mejor coordinación entre los diferentes ámbitos de seguridad, siempre que sea posible, las auditorías que se encarguen deberán analizar de forma conjunta los diferentes ámbitos de la seguridad que son objeto de la presente orden.

CAPÍTULO II

Política de Seguridad TIC

Artículo 17. 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.

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

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

00309996

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 con competencias en sistemas de información sectoriales de la Agencia Digital de Andalucía asignados 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 la Presidencia, Interior, Diálogo Social y Simplificación Administrativa
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 con competencias en sistemas de información sectoriales de la Agencia Digital de Andalucía asignado a la Consejería.

5. La Unidad de Seguridad TIC se encargará de la gestión de la documentación de referencia indicada, 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 18. 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 personales.

c) Delegado de Protección de Datos.

Artículo 19. 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 así el principio de función diferenciada recogido en el artículo 5.j) de dicho decreto, y contemplado asimismo en el artículo 11 del ENS. La Unidad de Seguridad TIC ejercerá las funciones de

00309996

Responsabilidad de Seguridad TIC de la Consejería, debiendo ser designada la persona responsable de la citada Unidad por el Comité de Seguridad Interior y Seguridad TIC de dicha Consejería, a propuesta de la Agencia Digital de Andalucía.

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 Interior y 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 realización y mantenimiento de los análisis de riesgos de la Consejería, bajo la supervisión de la persona que ostente la condición de Delegado de Protección de Datos.

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.

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 20. 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 21. 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 las personas Responsables de los Sistemas y de las personas Responsables de los Servicios.

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

00309996

d) Aceptar los riesgos residuales y realizar su seguimiento y control.

Artículo 22. Responsable del Sistema.

1. El Responsable del Sistema será la persona adscrita a la unidad administrativa 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 porque 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.

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 23. 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:

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.

d) Aceptar los riesgos residuales y realizar su seguimiento y control.

00309996

Artículo 24. 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 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 25. Función diferenciada.

De conformidad con lo previsto en el artículo 13.3 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 26. Clasificación y control de activos en materia de Seguridad TIC.

1. Los recursos informáticos y la información de la Consejería en base al ENS se encontrarán inventariados. Este inventario contará con una persona responsable, encargada de definir los criterios de seguridad asociados y, en caso de ser necesario, se definirá una persona para la custodia del recurso. Dicha persona encargada velará por cumplir los criterios de seguridad definidos por la persona responsable de los mismos. Los inventarios se mantendrán actualizados para asegurar su validez.

2. Los activos de información estarán clasificados de acuerdo con 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 27. 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 de 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 Interior y Seguridad TIC.

00309996

CAPÍTULO III

Política de Seguridad Interior

Artículo 28. Planificación de la Seguridad Interior.

La planificación de la Seguridad Interior en la Consejería se llevará a cabo en los términos recogidos en el artículo 17 del Decreto 171/2020, de 13 de octubre.

Artículo 29. 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:

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 30. Unidad de Seguridad Interior.

1. La Consejería, de acuerdo con lo establecido en el artículo 10 del Decreto 171/2020, de 13 de octubre, 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.

2. Tendrá las siguientes atribuciones, de acuerdo con lo dispuesto en el artículo 10.2 del Decreto 171/2020, de 13 de octubre:

a) Asesorar, informar y ofrecer soporte al Comité de Seguridad Interior y Seguridad TIC, así como la ejecución de sus decisiones y acuerdos en materia de seguridad interior. Elaboración de una Propuesta de un Plan de Seguridad Interior para la Consejería.

b) 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.

c) Desarrollar, mantener y supervisar el marco regulador de la seguridad interior en la Consejería.

d) Generar y supervisar los criterios y directrices para la gestión de la seguridad interior en el ámbito de la Consejería.

e) Recoger sistemáticamente la información y supervisar el estado de las principales variables de seguridad interior en el ámbito de la Consejería.

f) Coordinar y realizar el seguimiento de la actividad de los puntos coordinadores responsables de seguridad interior de la Consejería en cada provincia.

g) Asesorar técnicamente el sistema de seguridad interior en el ámbito de la Consejería.

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

i) Gestionar, para el ámbito de la Consejería, la relación con la Unidad Corporativa de Seguridad Interior.

j) 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 Consejería.

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

l) Asegurar, en el ámbito de la Consejería, 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.

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

n) Informar sobre incidentes de seguridad interior en la Consejería que se consideren relevantes.

00309996

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

o) Proponer a la aprobación del Comité de Seguridad Interior y Seguridad TIC el Plan de Seguridad Interior de la Consejería o entidad dependiente singular.

p) Cuantas otras le sean encomendadas en relación con la seguridad interior por el Comité de Seguridad Interior y Seguridad TIC.

3. La Unidad de Seguridad Interior, en el ejercicio de sus funciones, se coordinará con los órganos directivos centrales que tengan atribuidas competencias de gestión en relación con los diferentes activos a proteger.

4. A los efectos del adecuado cumplimiento de sus funciones, en la planificación de la seguridad interior se establecerán los mecanismos o instrumentos de comunicación inmediata y permanente de la Unidad de Seguridad Interior con los Puntos Coordinadores previstos en el artículo 30, así como con los distintos responsables que en esta materia y, de conformidad con lo previsto en el artículo siguiente, se establezcan en las Delegaciones de Gobierno.

Artículo 31. 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 32. Puntos Coordinadores de Seguridad Interior.

1. A nivel provincial, existirán Puntos Coordinadores de Seguridad Interior que serán asumidos por personal de las Delegaciones del Gobierno designados al efecto por el Comité de Seguridad a propuesta de las personas titulares de dichos órganos periféricos.

2. Las atribuciones y funciones de los Puntos Coordinadores de Seguridad Interior serán las contempladas en el artículo 13 del Decreto 171/2020, de 13 de octubre, así como aquellas que se entiendan precisas y se recojan dentro de los diferentes niveles de planificación o resulten necesarias en su implementación, atendiendo a los criterios establecidos por el Comité de Seguridad o la Unidad de Seguridad Interior.

Artículo 33. 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 34. 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 y en los demás instrumentos de planificación previstos en el artículo 17 del Decreto 171/2020, de 13 de octubre.

CAPÍTULO IV

Política de protección de datos personales

Artículo 35. Ámbito de aplicación.

Esta política de protección de datos personales de la Consejería será de aplicación a todos los tratamientos de datos personales que lleven los órganos de la misma en el ejercicio de las competencias que tenga 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.

00309996

Artículo 36. Responsables de los Tratamientos de datos personales.

1. Tendrán la consideración de Responsables de Tratamiento los órganos directivos de la Consejería que en el ejercicio de sus competencias realicen alguna actuación que conlleve el tratamiento de datos personales y determinen los fines y medios del mismo, salvo que las normas aplicables sobre asignación de atribuciones en materia de protección de datos personales dispongan otra cosa, según lo dispuesto en el art. 33 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

2. En el caso de los órganos directivos periféricos de la Consejería, los Responsables de los Tratamientos son las Delegaciones del Gobierno de la Junta de Andalucía en cada provincia, así como la Subdelegación del Gobierno en el Campo de Gibraltar, 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.

3. La condición de Responsable del Tratamiento coincidirá con la de Responsable de la Información.

4. Cada responsable del tratamiento de datos personales aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme a la normativa de protección de datos.

Artículo 37. Encargados de los Tratamientos de datos personales.

1. Cuando se vaya a realizar un tratamiento por cuenta del responsable del tratamiento, este elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas. 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. Los encargos de tratamiento deberán quedar reflejados en la memoria prevista en el artículo 39 de esta orden y se regirán por lo previsto en el artículo 28 del Reglamento General de Protección de Datos.

2. El Responsable del Tratamiento deberá formalizar con el Encargado de Tratamiento el contrato o acto jurídico previsto en el artículo 28.3 del Reglamento General de Protección de Datos. Para ello se estará a 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, protección de datos y otras materias.

3. 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 personales.

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.

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

Artículo 38. Delegado de Protección de Datos.

1. La Consejería contará con una persona que ostente la condición de Delegado de Protección de Datos a efectos de lo establecido en los artículos 37 a 39 del Reglamento

00309996

General de Protección de Datos, en los artículos 34 a 37 de la Ley Orgánica 3/2018, de 5 de diciembre, y, cuando sea de aplicación, en los artículos 40 a 42 de la Ley Orgánica 7/2021, de 26 de mayo.

2. Su ámbito de actuación se extenderá a las actividades de tratamiento de datos personales de los órganos de la Consejería que se lleven a cabo en el ejercicio de las competencias propias de la misma. 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.

3. La persona que ostente la condición de Delegado de Protección de Datos será designada por la persona titular de la Viceconsejería entre personal funcionario adscrito a la Consejería, no pudiendo ser removida ni sancionada por desempeñar sus funciones, salvo que incurriera en dolo o negligencia grave en su ejercicio. La resolución por la que se le designe determinará el ámbito respecto al cual ejercerá sus funciones. Ejercerá sus funciones con dedicación exclusiva, ocupará un puesto de trabajo con un complemento de destino de nivel 27, al menos. debiéndose garantizar su independencia dentro de la organización y evitar cualquier conflicto de intereses. Su designación, nombramiento y cese serán notificados al Consejo de Transparencia y Protección de Datos de Andalucía, en el plazo de diez días, de conformidad con los artículos 37.7 del Reglamento General de Protección de Datos y 34.3 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

4. Son funciones de la persona que ostente la condición de Delegado de Protección de Datos, además de la supervisión del cumplimiento de la política de protección de datos de la Consejería, las establecidas en los artículos 35.2 y 39.1 del Reglamento General de Protección de Datos, en los artículos 36.1 y 4, 37 y 65.4 de la Ley Orgánica 3/2018, de 5 de diciembre, y, en su caso, en los artículos 41. 1 y 4 y 42 de la Ley Orgánica 7/2021, de 26 de mayo.

Artículo 39. 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 ya citado. 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 en cuáles actúa como responsable y en cuáles actúa 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 que ostente la condición de Delegado 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 del Gobierno de la Junta de Andalucía en cada provincia, se registrarán de manera uniforme y se publicarán conjuntamente en el Inventario de Actividades de Tratamiento de la

00309996

Administración de la Junta de Andalucía. El resto de las actividades de tratamiento que sean específicas de alguna Delegación del Gobierno de la Junta de Andalucía concreta se registrarán y publicarán separadamente.

Artículo 40. Ejercicio de derechos en materia de protección de datos personales.

1. Mediante Instrucción de la Viceconsejería se 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 las obligaciones impuestas a los responsables de tratamiento por la normativa que resulte de aplicación, así como el modo de proceder para atender a las solicitudes presentadas.

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 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 41. 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 25.2 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, convenio, 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 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.

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 en la Protección de Datos personales.

00309996

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 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, previsto en el artículo 15.1.d) del Decreto 434/2015, de 29 de septiembre, por el que se aprueban los Estatutos del Consejo de Transparencia y Protección de Datos de Andalucía. Se podrá consultar a la persona que ostente la condición de Delegado de Protección de Datos si, a su juicio, un determinado anteproyecto de ley o proyecto de disposición de carácter general pudiera afectar a la materia de protección de datos hasta el punto de ser preceptivo o recomendable la solicitud del mencionado 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 de Protección de Datos, en la fase de diseño del proyecto, antes de adquirirse compromisos contractuales y económicos.

Artículo 42. 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, 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, cuando resulten agravadas respecto de las previstas en el Esquema Nacional de Seguridad.

Artículo 43. 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 documentos 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

00309996

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 de 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 del Gobierno.

Artículo 44. 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, por cada actividad de tratamiento de datos, un análisis de riesgo para los derechos y libertades de las personas interesadas, atendiendo a la naturaleza, el ámbito, el contexto y los fines de la actividad de tratamiento.

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 45. Evaluación de Impacto en la Protección de Datos (EIPD).

1. Cuando sea probable que 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), de conformidad con el artículo 35 del Reglamento General de Protección de Datos y el resto de normativa aplicable, así como seguir el protocolo aprobado de acuerdo con el artículo 48.1.c) de la presente orden. Para ello, recabará el asesoramiento de la persona que ostente la condición de Delegado 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

00309996

suscrita por la persona titular del órgano responsable del tratamiento. La persona que ostente la condición de Delegado de Protección de Datos dará traslado de la misma a la autoridad de control.

Artículo 46. Violaciones de la seguridad de datos personales.

1. Se aprobará 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 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 realización de una valoración del riesgo que conlleva la violación de seguridad para los derechos y libertades de las personas físicas.

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

d) 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.

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

f) 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 y, de ser posible, en un plazo máximo de 72 horas desde 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.

Artículo 47. Formación, concienciación y sensibilización.

El órgano competente en materia de formación del personal de la Consejería, con el asesoramiento de la persona que ostente la condición de Delegado 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 48. Protocolos e Instrucciones.

1. Se establecerán 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.

b) Protocolo sobre gestión de violaciones de la seguridad de datos personales.

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

00309996

deberán incorporar cualquier aspecto que sea necesario o aconsejable desde el punto de vista de la normativa en materia de protección de datos.

Artículo 49. 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 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, 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 de Protección de Datos, en su condición de interlocutor ante 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 como de la respuesta dada por la misma a la reclamación presentada por un afectado, dentro del procedimiento establecido en el artículo 37.2 en relación con el artículo 65.4, ambos de la Ley Orgánica 3/2018, de 5 de diciembre. Asimismo, 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 por ausencia, vacante o enfermedad del Delegado de Protección de Datos.

Artículo 50. 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.

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 y del Comité de Seguridad Interior y TIC, así como del Delegado 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.

00309996

Disposición derogatoria única. Derogación normativa.

Queda derogada la Orden de 30 de agosto de 2018, por la que se establece la política de la seguridad de las tecnologías de la información y telecomunicaciones, así como el marco organizativo y tecnológico en el ámbito de la Consejería de la Presidencia, Interior, Diálogo Social y Simplificación Administrativa, así como cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en esta orden.

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 el día siguiente al de su publicación en el Boletín Oficial de la Junta de Andalucía.

Disposición final tercera. Publicidad de la política de seguridad de la Consejería.

A los efectos de su mejor difusión entre las personas empleadas de la organización y de otras partes interesadas, la presente orden se publicará, además de en el Boletín Oficial de la Junta de Andalucía, en el portal web y medios de difusión internos (Intranet) de la Consejería y sus entes instrumentales y en la sección de transparencia del Portal de la Junta de Andalucía, sin perjuicio de las obligaciones previstas en el artículo 13 de la Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía y en los medios y soportes que se establezcan por el Comité de Seguridad Interior y Seguridad TIC.

Sevilla, 23 de octubre de 2024

ANTONIO SANZ CABELLO
Consejero de la Presidencia, Interior, Diálogo Social
y Simplificación Administrativa

00309996