ORDEN DE XXXXXX DE 2025, POR LA QUE SE ESTABLECE LA POLÍTICA DE SEGURIDAD INTERIOR, SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES Y DE LA PROTECCIÓN DE DATOS PERSONALES DE LA CONSEJERÍA DE TURISMO Y ANDALUCÍA EXTERIOR. (BORRADOR INICIAL 01/07/25)

La presente orden, de carácter organizativo y con efectos internos, se dicta en aplicación del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Respecto a la Seguridad en las TIC, el Consejo de Gobierno de 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, obligando a las distintas Consejerías a disponer de su propio documento de política de Seguridad TIC.

En relación con la Seguridad Interior, el Decreto 171/2020, de 13 de octubre, establece la política de Seguridad Interior en la Administración de la Junta de Andalucía, regulando en su Capítulo II un modelo organizativo funcional, actualizando las respectivas normas de creación de los Comités a los que alude el artículo 10 del Decreto 1/2011, de 11 de enero. El citado Decreto dispone 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.

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 del Decreto 171/2020, de 13 de octubre.

Sobre la Protección de datos de carácter personal, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, de la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante Reglamento General de Protección de Datos, RGPD) dispone que todo tratamiento de datos personales se debe llevar a cabo atendiendo al principio de responsabilidad proactiva que, entre otras implicaciones, incluye la necesidad de que quien determine los fines y medios del tratamiento adopte medidas técnicas y organizativas para garantizar la seguridad adecuada al riesgo de los tratamientos de datos personales.

En cuanto a los principios relativos al tratamiento de datos personales, el artículo 5.1.f) del RGPD regula el de integridad y confidencialidad, determinando que serán tratados de tal manera que se garantice una seguridad adecuada, tanto en su recogida, como en su explotación, conservación y destrucción, mediante la aplicación de medidas técnicas u organizativas apropiadas.

En la elaboración de esta orden se ha tenido en cuenta también la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. 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 2018/1972/UE.

Además, el Real Decreto 311/2022, de 3 de mayo, cuyo objeto es determinar la política de seguridad en la utilización de medios electrónicos, establece los principios básicos y los requisitos mínimos que permitan 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.

El artículo 12 de dicho Real Decreto 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 la mencionada norma.

Conforme establece el artículo 156.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, el Esquema Nacional de Seguridad tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la presente Ley, y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada.

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, aprobados mediante Decreto 128/2021, de 30 de marzo, por el que se aprueban los Estatutos de la Agencia Digital de Andalucía.

El Decreto del Presidente 6/2024, de 29 de julio, sobre reestructuración de Consejerías, creó la Consejería de Turismo y Andalucía Exterior, estableciendo en su artículo 5 las competencias que se le atribuyen. Para el ejercicio de estas, el Decreto 166/2024, de 26 de agosto, establece la estructura orgánica de la Consejería.

Mediante Orden del entonces Consejero de Turismo, Cultura y Deporte de 15 de noviembre de 2023, se establecía la política de seguridad de la extinta Consejería de Turismo, Cultura y Deporte en los ámbitos de seguridad interior, seguridad de las tecnologías de la información y comunicaciones y de la protección de datos personales.

Como consecuencia de lo expuesto y, en el ámbito de las competencias asumidas ahora por la Consejería de Turismo y Andalucía Exterior, con el objetivo de crear el marco necesario y las condiciones imprescindibles para garantizar la seguridad y confianza en el ejercicio de las competencias que le son propias a esta Consejería, la presente orden tiene la finalidad de establecer la política de seguridad de la Consejería de Turismo y Andalucía Exterior, englobando los tres ámbitos materiales que requieren de una actividad proactiva y preventiva por parte de la Administración, tales como, la seguridad en el ámbito de las TIC, la seguridad interior y la seguridad relativa a la protección de datos de carácter personal, estableciendo la estructura de organización y gestión, y desarrollando las directrices y principios básicos que deben regir las actuaciones en todas estas materias de seguridad.

Esta orden consta de cuarenta y ocho artículos, distribuidos en cinco capítulos, tres disposiciones adicionales, una disposición derogatoria única y dos disposiciones finales.

El Capítulo I contiene disposiciones generales sobre el objeto de la norma y su ámbito de aplicación, así como las definiciones, objetivos y principios que regirán la política de seguridad de la Consejería.

El Capítulo II se refiere a la organización de la política de seguridad. Contiene la estructura organizativa, la regulación del Comité de Seguridad Interior y Seguridad TIC de la Consejería de Turismo y Andalucía Exterior, 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 obligaciones del personal y la resolución de conflictos en los distintos ámbitos aludidos en la presente orden.

El Capítulo III, sobre la Política de Seguridad TIC de esta Consejería, regula la estructura organizativa de la gestión de seguridad TIC.

El Capítulo IV, relativo a la Política de Seguridad Interior de esta Consejería, establece la estructura organizativa de la gestión de la seguridad interior en la misma.

El Capítulo V está dedicado a la política de Protección de Datos de Carácter Personal. Además de asumir la incidencia de los aspectos fundamentales del Reglamento General de Protección de Datos, recoge sus figuras fundamentales, como son el Responsable del Tratamiento, el Encargado del Tratamiento y el Delegado de Protección de Datos, en la política de seguridad TIC y Seguridad Interior de la Consejería.

La presente Orden cumple con los principios de buena regulación establecidos en el artículo 129 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

En cuanto a los principios de necesidad y eficacia, se dicta por razones de interés general, por cuanto resulta imprescindible establecer la política de seguridad de la Consejería de Turismo y Andalucía Exterior, y regular los elementos organizativos y procedimentales necesarios 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 a sus destinatarios y evita imponer cargas administrativas adicionales, por su carácter organizativo e interno, a la ciudadanía y a las empresas, limitándose a utilizar los recursos ya existentes para dar los servicios requeridos sin que suponga ningún incremento de gasto. Por lo que se refiere 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, la competencia para aprobar esta norma está atribuida a la persona titular de la Consejería, de conformidad con el ejercicio de la potestad reglamentaria previsto en el artículo 44.2 de la Ley 6/2006, de 24 de octubre, del Gobierno de la Comunidad Autónoma de Andalucía, y su rango, según dispone el artículo 46.4, debe ser el de orden. Asimismo, se han tenido en cuenta todas las normas europeas, estatales y autonómicas de aplicación, generando

un marco normativo adecuado que aporta claridad y certidumbre en relación con la política de seguridad de la Consejería, facilitando así su conocimiento y comprensión.
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 el artículo 133.4 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y en el artículo 28.2 de la Ley 7/2017, de 27 de diciembre, de Participación Ciudadana de Andalucía.

Asimismo, siendo uno de los objetivos de la Comunidad Autónoma Andaluza el de promover una sociedad igualitaria entre mujeres y hombres, en la elaboración de esta Orden se ha tenido en cuenta la integración transversal del principio de igualdad de género, de conformidad con lo establecido en 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.

Por otro lado, en la tramitación del presente proyecto normativo se han solicitado los informes preceptivos a que debe someterse el proyecto en su tramitación, de conformidad con lo previsto en el artículo 45.2 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, del Gobierno de la Comunidad Autónoma de Andalucía, 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 166/2024, de 26 de agosto,

DISPONGO

CAPÍTULO I
Disposiciones generales

Artículo 1. *Objeto.*

1. En aplicación del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, la presente orden tiene por objeto establecer la política de seguridad de la Consejería de Turismo y Andalucía Exterior (en adelante la 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 normativo del 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 (Reglamento General de Protección de Datos, RGPD), y de 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, aún no estando adscrita a la Consejería, tengan acceso a la información gestionada por la Consejería o 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 mientras no dispongan de una Política de Seguridad Interior propia.

4. La Política de Protección de Datos Personales se aplicará a todas las actividades de tratamiento 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. Asimismo, deberá ser observada por todo el personal destinado en dichos órganos y unidades administrativas, así como por aquellas personas que, no estando adscritas a la Consejería, tengan acceso a la información gestionada por la Consejería o a sus sistemas de información.

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 de carácter personal 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 (RGPD); 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 de carácter Personal de la Consejería se adopta como medida de responsabilidad proactiva demostrable, proporcionada al 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 de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía y en el Esquema Nacional de Seguridad (ENS) 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 Consejería se desarrollará, con carácter general, de acuerdo con los siguientes principios:

a) Anticipación y prevención.

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

c) Preservación de la resiliencia.

d) Unidad de acción, coordinación y colaboración.

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

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

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

h) Aseguramiento de la continuidad de los servicios.

i) Responsabilidad estratificada, identificable y compartida.

j) Actuación planificada.

Artículo 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.

CAPÍTULO II
Organización de la Política de Seguridad

Artículo 9. ***Estructura organizativa***

1. La política de seguridad de la Consejería se conforma mediante la siguiente estructura organizativa mínima:

a) El Comité de Seguridad Interior y Seguridad de las Tecnologías de la Información y las Comunicaciones (en adelante Comité de Seguridad Interior y Seguridad TIC), que no tendrá carácter colegiado, actuará como órgano de dirección y seguimiento de la política de seguridad de la Consejería.

b) Grupo de respuesta a incidentes en los sistemas de información, con función de toma urgente de decisiones en caso de contingencia grave.

c) Unidad de Seguridad TIC, cuya persona titular tendrá la condición de Responsable de Seguridad TIC de la Consejería.

d) Responsables de la Información.
e) Responsables del Sistema.
f) Responsables del Servicio.
g)Delegado o Delegada de Protección de Datos.
h) Responsables de los Tratamientos de Datos personales.
i) Encargados de los Tratamientos de Datos Personales.

j) Unidad de Seguridad Interior, cuya persona titular tendrá la condición de Responsable de Seguridad Interior de la Consejería.

k) Puntos Coordinadores de Seguridad Interior.

l) Responsables de Seguridad de activos, conforme a lo que se establezca en los instrumentos de planificación previstos en el Decreto 171/2020, de 13 de octubre, teniendo en cuenta la definición del concepto de activo previsto en su Anexo I.

2. En función de las necesidades y circunstancias de la organización, los cometidos de varios de estos perfiles podrán ser asumidos por una misma persona o grupo de personas, unidad administrativa o departamento. Las funciones del responsable del tratamiento también podrán recaer en un órgano administrativo de los definidos en el artículo 5 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, y en los artículos 13 y 16 de la Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía.

No obstante, en todo caso, se deberá garantizar que la responsabilidad de la seguridad de las TIC esté diferenciada de la responsabilidad que es propia a la prestación de los servicios.

3. Este modelo organizativo, sin perjuicio de lo previsto en el artículo siguiente, tiene el carácter de mínimo. Las propuestas de nuevas estructuras o perfiles de seguridad deberán ser remitidas, para su estudio y aprobación, al Comité de Seguridad Interior y Seguridad TIC,

especificando las funciones que se le asignarán y, en caso de perfiles, las competencias requeridas para su desempeño, debiendo ser aprobada su creación por acuerdo de este Comité de Seguridad.

Artículo 10. *Comité de Seguridad Interior y Seguridad TIC*

1. La Consejería, atendiendo a lo establecido en el artículo 10 del Decreto 1/2011, de 11 de enero, contará con un Comité de Seguridad Interior y Seguridad TIC, como órgano que desarrollará la dirección y seguimiento en materia de seguridad de la información y de los activos TIC y del tratamiento de datos personales de los que la Consejería sea titular a través del correspondiente responsable de la información, del servicio o del tratamiento, 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 el seguimiento en materia de seguridad interior.

Corresponde a la persona titular de la Secretaría General Técnica su impulso y organización, así como velar por su buen funcionamiento.

2. El Comité de Seguridad Interior y Seguridad TIC de la Consejería estará formado por las siguientes personas:

a) Presidencia: La persona titular de la Viceconsejería.

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

c) Vocalías:

1º La persona titular de cada uno de los órganos directivos centrales de la Consejería que tenga responsabilidad sobre algún activo, tratamiento, información, servicio y/o sistema.

2º Las personas titulares de las Coordinaciones Generales de la Viceconsejería y de la Secretaría General Técnica.

3º La persona que ostente la representación legal de cada una de las entidades vinculadas o dependientes.

4º Las personas encargadas de la seguridad TIC de la Empresa Pública para la Gestión del Turismo y el Deporte en Andalucía, S.A., de la Sociedad Red de Villas Turísticas de Andalucía, S.A. y de La Fundación Real Escuela Andaluza de Arte Ecuestre.

5º Las personas responsables de la Unidad de Seguridad TIC, de la Unidad de Seguridad Interior y la que ostente la condición de Delegado o Delegada de Protección de Datos, asistirán en calidad de personas asesoras a las reuniones del Comité, salvo que puntualmente se disponga lo contrario de forma expresa por parte de la presidencia. El Comité podrá convocar a sus reuniones a las personas que en cada caso autorice la presidencia, por propia iniciativa o a propuesta de cualquiera de sus miembros. Así mismo podrá recabar del personal técnico especializado, propio o externo, la información pertinente para la toma de decisiones.

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 designada por el Comité de Seguridad Interior y Seguridad TIC, sin que resulte exigible la adscripción funcional a la Consejería. Ejercerá las funciones propias de dicho cargo, entre otras, las de convocar las reuniones por orden de la persona titular de la presidencia, preparar el Orden del día de las mismas y elaborar el acta de las sesiones. Su designación será acordada por el conjunto de miembros de dicho comité, por un plazo máximo de cuatro años, prorrogable, una sola vez, por otros cuatro años.

3. En la composición, modificación o renovación del Comité de Seguridad Interior y Seguridad TIC se garantizará, en la medida de lo posible, la representación paritaria de mujeres y hombres, conforme a lo establecido en el artículo 19.2 de la Ley 9/2007, de 22 de octubre, y a la

definición de representación equilibrada contenida en el artículo 3.3 de la Ley 12/2007, de 26 de noviembre, para la Promoción de la Igualdad de Género en Andalucía.

4. 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 y la secretaría podrán designar a una persona suplente, con carácter permanente y aplicando un criterio de paridad entre mujeres y hombres, de entre personal funcionario a su servicio, dando preferencia al personal funcionario con formación o experiencia en las materias sobre las que el Comité de Seguridad Interior y Seguridad TIC ejerce sus funciones. Dicha designación será comunicada a la Secretaría.

5. En todo lo no dispuesto por este artículo, el Comité de Seguridad Interior y Seguridad TIC se regirá por lo previsto en esta Orden, por la normativa reguladora de la política de seguridad en la Administración de la Junta de Andalucía, así como por el resto de la normativa aplicable, la reguladora del Esquema Nacional de Seguridad (ESN) y la de protección de datos personales.

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

Serán funciones propias del Comité de Seguridad Interior y Seguridad TIC:

a) Aprobar el desarrollo de la política de seguridad TIC de segundo nivel, de seguridad interior, de protección de datos personales y de las resoluciones que se aprueben por parte del órgano directivo central competente en materia de coordinación y ejecución de las políticas de seguridad de los sistemas de información y telecomunicaciones de la Administración de la Junta de Andalucía, de conformidad con el artículo 2.5 de la Orden de la Consejería de Empleo, Empresa y Comercio de 9 de junio de 2016, por la que se efectúa el desarrollo de la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía.

b) Establecer directrices comunes y de supervisión del cumplimiento de la normativa en materia de seguridad interior, de seguridad TIC y de protección de datos personales.

c) Definir, aprobar y realizar el seguimiento de los objetivos, iniciativas y planes estratégicos en materia de seguridad interior, incluido el Plan de Seguridad Interior, de la seguridad TIC y de la protección de datos personales, así como promover la dotación de recursos necesarios para el cumplimiento de dichas iniciativas y planes.

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

e) Aprobar el modelo de relación con los Puntos Coordinadores de Seguridad Interior.

f) Velar, dentro de los límites establecidos en los programas asignados por las leyes anuales de presupuestos a la Consejería, porque los medios y recursos necesarios para posibilitar la realización de las iniciativas planificadas y de los planes estratégicos definidos, sean proporcionados. Entre ellas, la evaluación por parte de la Unidad de Seguridad TIC de los aspectos de seguridad de nuevos sistemas de información o de evolutivos de los existentes, antes de su puesta en producción, como se recoge en el artículo 11.1.e) del Decreto 1/2011, de 11 de enero.

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

h) Nombrar a los miembros de la Unidad de Seguridad Interior y a los miembros de la Unidad de Seguridad TIC de la Consejería, así como a las personas que asuman la responsabilidad de cada una de ellas. Igualmente nombrará a las personas responsables en materia de seguridad interior de las entidades adscritas a la Consejería.

Asimismo, le corresponderá nombrar a los Responsables del Sistema y a las personas que en las Delegaciones Territoriales de la Consejería asuman los Puntos Coordinadores de Seguridad.

i) 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.

j) Promover, aprobar y realizar el seguimiento de la planificación de auditorías periódicas para verificar el correcto cumplimiento de la política, la normativa y los procedimientos de seguridad.

k) Aprobar las medidas correctoras que correspondan derivadas de las conclusiones elaboradas por la Unidad de Seguridad TIC, la Unidad de Seguridad Interior o por el Delegado o Delegada de protección de datos, a partir de su actividad o de los resultados de una auditoría.

l) Promover y fomentar la divulgación y formación en materia de seguridad interior, seguridad TIC y en los principios relativos al tratamiento de datos personales, 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. Así como promover la formación continua y especializada de los miembros de la Unidad de Seguridad Interior, de la Unidad de Seguridad TIC y del Delegado o Delegada de Protección de Datos.

m) Planificar y priorizar las iniciativas necesarias para cumplir con las directrices, los objetivos y los principios básicos marcados en la política de seguridad regulada en la presente Orden. En especial, la elaboración, actualización y evaluación periódica de los análisis de riesgos necesarios.

n) Impulsar los preceptivos análisis de riesgos junto a la Unidad de Seguridad Interior, o la Unidad de Seguridad TIC y los perfiles Responsable de la Información, Responsable del Servicio y Delegado o Delegada de Protección de Datos. Para ello, se deberá impulsar la determinación de los niveles de seguridad de la información tratada y de los servicios prestados, usando la valoración de los impactos que tendrían los incidentes que afectaran a la política de seguridad.

ñ) Gestionar la aceptación de los riesgos residuales por sus responsables correspondientes respecto de la información y de los servicios de su competencia, obtenidos en el análisis de riesgos.

o) Monitorizar el desarrollo del proceso de gestión de incidentes de seguridad, así como la toma de decisiones en respuesta a incidentes de seguridad críticos.

p) Establecer los mecanismos necesarios de coordinación de los diferentes órganos de seguridad de las entidades vinculadas o dependientes de la Consejería.

q) Proponer a los Responsables del tratamiento las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad, de acuerdo con el correspondiente análisis de riesgo para los derechos y libertades de las personas físicas y, en su caso, las evaluaciones de impacto en la protección de datos personales, contando con el asesoramiento del Delegado o Delegada de Protección de Datos.

r) Cuantas otras le sean encomendadas.

Artículo 12. ***Régimen de funcionamiento del Comité de Seguridad Interior y Seguridad TIC***

1. El Comité de Seguridad Interior y Seguridad TIC se reunirá de forma ordinaria, al menos, una vez al año. También podrá celebrar reuniones extraordinarias a petición propia o previa solicitud razonada de sus miembros, si se produjeran incidentes de seguridad graves o se

produjeran conflictos que pudieran afectar gravemente a los servicios prestados por la Consejería.

Asimismo, se podrán celebrar reuniones extraordinarias en caso de modificaciones sustanciales del marco normativo de seguridad interior, seguridad TIC y protección de datos personales o de los riesgos a los que se encuentren expuestos los sistemas de información.

La evaluación de la oportunidad y conveniencia para convocar una reunión extraordinaria la realizará la persona titular de la vicepresidencia del mencionado Comité, que lo someterá a la presidencia del mismo. Todas las reuniones se realizarán previa convocatoria.

2. El Comité de Seguridad Interior y Seguridad TIC podrá ser convocado, celebrar sus sesiones, adoptar acuerdos y aprobar y remitir actas, tanto de forma presencial como telemática, 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 transmitida, de conformidad con lo establecido en el artículo 91.3 de la Ley 9/2007, de 22 de octubre.

Las personas miembros del Comité de Seguridad Interior y Seguridad TIC están obligadas a respetar la confidencialidad de toda la información a la que tengan acceso.

3. El Comité de Seguridad Interior y Seguridad TIC 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 Esquema Nacional de Seguridad y las normativas de seguridad interior y de protección de datos personales.

4. Cuando el tratamiento de determinadas cuestiones así lo requiera, se podrá convocar a las reuniones de este Comité de Seguridad Interior y Seguridad TIC al personal técnico especializado, propio o externo, a los efectos de prestar asesoramiento experto, estando obligados a respetar la confidencialidad de toda la información a la que tengan acceso, sin que en ningún caso pueda ocasionar coste económico.

5. La persona que ostente la secretaría del Comité de Seguridad Interior y Seguridad TIC levantará acta de cada reunión del mismo.

6. El Comité de Seguridad Interior y Seguridad TIC establecerá entre sus miembros un Grupo de Respuesta a Incidentes de Seguridad de la información que requieran una respuesta urgente y coordinada, y definirá sus normas básicas de funcionamiento.

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 principal será la toma urgente de decisiones en caso de contingencia grave que afecte a la seguridad de los activos o 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 la persona titular de la presidencia del Comité de Seguridad Interior y Seguridad TIC contando con el apoyo de la persona Responsable de la Unidad de Seguridad TIC de la Consejería, de la persona Responsable de la Unidad de Seguridad Interior de la Consejería, de la persona que ostente la condición de Delegado o Delegada de Protección de Datos, y, en su caso, de las personas responsables de otras Unidades de Seguridad. 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 redes y sistemas de información, concretamente a su equipo de respuesta a incidentes de seguridad informática (SOC Andalucía, CSIRT o CERT), los incidentes de seguridad TIC, en los casos y en los términos que determine la normativa aplicable.

4. La notificación mencionada en el apartado anterior 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. La preservación de la seguridad, en los tres ámbitos que se regulan en la presente orden, será considerada objetivo común de todas las personas al servicio de los órganos y entidades vinculadas o dependientes incluidos en el ámbito de aplicación de esta norma, siendo éstas responsables del uso correcto de la información a la que tengan acceso, de los activos que se vean involucrados en sus tareas durante el desempeño ordinario de sus funciones y actividades, así como de la detección precoz de cuantos indicios puedan servir a la prevención de riesgos para la seguridad de la información y la seguridad interior.

2. Todas las personas empleadas que presten servicios en la Consejería o en sus entidades vinculadas o dependientes tienen la obligación de conocer y cumplir la política de seguridad de la Consejería y las normas que le son de general aplicación, siendo responsabilidad del Comité de Seguridad Interior y de Seguridad TIC establecer los mecanismos adecuados para que la información llegue a las personas afectadas.

3. Con carácter general, para el personal de la Consejería y de las entidades vinculadas o dependientes de la misma, regirán las normas de uso de los recursos TIC atendiendo al 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, así como a cualesquiera otras instrucciones y normas que regulen el comportamiento de las personas empleadas públicas en el uso de los sistemas informáticos y redes de comunicaciones de ésta.

4. Procederá el ejercicio de las acciones pertinentes para la exigencia de las responsabilidades legales que correspondan por el incumplimiento manifiesto de la política de seguridad TIC, Seguridad Interior o de la normativa de seguridad derivada, y en materia de protección de datos personales.

5. Cualquier persona física o jurídica que actúe bajo la autoridad del Responsable de un Tratamiento de datos personales en el ámbito de aplicación de la presente Orden y tenga acceso a datos personales, solo tratará dichos datos respetando las instrucciones del Responsable del Tratamiento, en cumplimiento del ordenamiento jurídico comunitario, nacional o autonómico.

6. Los responsables y encargados del tratamiento de datos así como todas las personas que intervengan en cualquier fase de este estarán sujetas al deber de confidencialidad al que se refiere el artículo 5.1.f) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, obligación que será complementaria al deber de secreto profesional. Estas obligaciones se mantendrán aún cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento.

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 serán resueltos por el 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 de carácter personal. En cualquier caso, cuando la persona o personas que asuman la figura del Delegado o Delegada de Protección de Datos aprecien la existencia de una vulneración relevante en materia de protección de datos lo documentará y lo comunicará inmediatamente al órgano directivo que tenga la condición de responsable o al encargado del tratamiento.

3. A los apartados anteriores les será aplicable el artículo 110 de la Ley 9/2007, de 22 de octubre.

CAPÍTULO III
Políticas de Seguridad TIC

Artículo 16. ***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 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 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 Turismo y Andalucía Exterior
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.

6. Conforme al artículo 2.4 de la Orden de la Consejería de Empleo, Empresa y Comercio de 9 de junio de 2016, por la que se efectúa el desarrollo de la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía, los procedimientos y guías técnicas tendrán carácter de recomendaciones y serán desarrollados con arreglo a los ámbitos en materia de seguridad de la información que se establezcan.

Artículo 17. ***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 la Unidad de Seguridad TIC, garantizando el principio de función diferenciada recogido en el artículo 5.j) de dicho Decreto, y contemplado asimismo en el artículo 11 del Esquema Nacional de Seguridad.

2. La persona titular de la Unidad de Seguridad TIC será designada, entre personal funcionario, por el Comité de Seguridad Interior y Seguridad TIC a propuesta de la persona titular del órgano directivo de la Agencia Digital de Andalucía que tenga atribuidas las competencias relacionadas con la estrategia y aplicación de las tecnologías de la información y de las comunicaciones.

3. La Unidad de Seguridad TIC de la Consejería tendrá las siguientes atribuciones:

a) Prestar soporte, asesoramiento e información a los responsables de la estructura de seguridad de la Consejería y al Comité de Seguridad Interior y Seguridad TIC, así como ejecutar las decisiones y acuerdos adoptados por éste.

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

c) Definir, Implantar y mantener los controles de carácter organizativo para la protección de los datos, aplicaciones y sistemas, así como la realización, supervisión y mantenimiento de los análisis de riesgos de la Consejería y la propuesta de las medidas necesarias para su tratamiento.

d) Revisar los análisis de riesgos de forma periódica, cuando existan cambios sustanciales en la información tratada o los servicios prestados, ocurra un incidente de seguridad grave o se reporten vulnerabilidades graves. A estos efectos, elaborará un listado de medidas organizativas y técnicas a implantar en la Consejería y lo elevará al Comité de Seguridad para su revisión y, en su caso, aprobación final.

Las funciones detalladas en las letras c) y d) de este apartado 3 se desempeñarán con el asesoramiento del Delegado o Delegada de Protección de Datos, de acuerdo con lo previsto en el artículo 3.2 del Real Decreto 311/2022, de 3 de mayo, y con el contenido de los requisitos de protección de la información sobre datos personales contemplado en el apartado 5.7.1 del Anexo II del citado Real Decreto.

e) Analizar los informes de auditorías, elevando al Comité de Seguridad Interior y Seguridad TIC las conclusiones.

f) Supervisar, de forma sistemática, los controles de carácter procedimental, operacional y medidas técnicas de protección de los datos, aplicaciones y sistemas de la Consejería.

g) Definir y supervisar 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 TIC, que incluye la definición de los requisitos y cláusulas de seguridad de los contratos de nuevos desarrollos, que deben estar actualizados en todo momento.

Adicionalmente, 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 a las personas responsables de la Información y responsables de los servicios correspondientes.

h) Elaborar y emitir un informe cuando, en el marco de una relación establecida con un tercero, éste no pueda satisfacer algún aspecto de la política de seguridad. El informe deberá precisar los riesgos en que se incurre y la forma de tratarlos, requiriendo la aceptación, en su caso, de las personas responsables de la información y responsables de los servicios afectados para continuar con la mencionada relación. Los referidos responsables deberán responder al informe en un plazo no superior a 30 días.

i) Definir y ejecutar los programas formativos y de concienciación relacionados con buenas prácticas de seguridad TIC en el ámbito de la Consejería.

j) Coordinar, dirigir y realizar seguimiento de la actividad en materia de seguridad TIC de las entidades vinculadas o dependientes de la Consejería, desde el momento en que se apruebe la política de seguridad de dichas entidades.

k) Velar por la aplicación de los criterios y directrices de gestión de la seguridad TIC emanadas de la Unidad de Seguridad TIC de la Junta de Andalucía.

l) Gestionar la documentación de seguridad TIC.

m) Determinar la categoría del sistema, según el Esquema Nacional de Seguridad, tomando como base las valoraciones de impacto realizadas por los Responsables de la Información y los Servicios afectados en dicho sistema.

n) Cuantas otras le sean encomendadas

4. La Unidad de Seguridad TIC realizará labores de apoyo a los Responsables del Tratamiento en la aplicación de medidas técnicas que sean competencia de dichos responsables.

Entre dichas labores se incluirá la ejecución de análisis de riesgos para los derechos y libertades de las personas físicas, interviniendo el Delegado o Delegada de Protección de Datos para el asesoramiento y la supervisión en la materia.

5. La Unidad de Seguridad TIC elaborará y mantendrá un inventario de servicios y sistemas, con indicación expresa de las personas u órganos que asumen las figuras de Responsable de la Información, Responsable del Tratamiento, Responsable del Servicio, Encargado del Tratamiento, Responsable del Sistema y Responsable de Seguridad TIC, para cada uno de ellas. Dicho inventario se entregará, actualizado, al Comité de Seguridad en cada una de sus reuniones, con indicación de aquellas deficiencias o faltas de información que se produzcan, de modo que el Comité de Seguridad disponga de información completa y pueda arbitrar los mecanismos necesarios para la subsanación de las deficiencias o faltas de información.

6. La Unidad de Seguridad TIC podrá ejercer como Responsable de Seguridad TIC de las entidades vinculadas o dependientes de la Consejería si es nombrada como tal por el Comité de Seguridad, previo informe favorable del órgano directivo del que dependa jerárquicamente dicha Unidad.

7. La Unidad de Seguridad TIC mantendrá un registro actualizado de las normas aplicables a la Consejería en materia de seguridad TIC y de protección de datos personales. Para ello, la Unidad de Seguridad TIC actuará de forma coordinada con el Delegado o Delegada de Protección de Datos.

Artículo 18. ***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 19. ***Responsables de la Información***

1. Los Responsables de la Información serán los órganos directivos que determinarán los requisitos de la información tratada. En el caso de los órganos directivos periféricos de la Consejería, los Responsables de la Información serán las Delegaciones Territoriales.

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

3. Los Responsables de la Información tendrán las funciones que establece para ellos el Esquema Nacional de Seguridad y, en particular, 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 Responsables de los Servicios y Responsables de los Sistemas afectados.

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.

4. Como responsable del tratamiento, además de las funciones descritas en el apartado anterior, le corresponderá adoptar la decisión sobre la creación del tratamiento, su finalidad, así como el contenido y uso de los datos tratados a lo largo de todo el ciclo de vida del tratamiento.

La información actualizada de dicho responsable junto a sus tratamientos se recogerá en el Registro de Actividades de Tratamiento de la Consejería a que hace referencia el artículo 38.

Artículo 20. ***Responsable del Sistema***

1. El Responsable del Sistema será la persona adscrita a la unidad administrativa que por sí misma 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. 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, incluyendo la definición de especificaciones, instalación y verificación de su correcto funcionamiento.

b) Velar 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 de información 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) Crear, mantener y actualizar de manera continua 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 tipología y sistema de gestión de los sistemas de información estableciendo los criterios de uso y los servicios disponibles en el mismo.

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

f) Acordar, en caso necesario, la suspensión del manejo de determinada información o la prestación de un determinado servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser consensuada con los Responsables de la Información afectada, del Servicio afectado y con la Unidad de Seguridad TIC, antes de ser ejecutada.

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

i) Investigar los incidentes de seguridad que afecten al sistema, y en su caso, comunicarlos al responsable de seguridad TIC o a quién éste determine.

Artículo 21. ***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. En el caso de los órganos directivos periféricos de la Consejería, los Responsables del Servicio serán las Delegaciones Territoriales.

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 Responsables de la Información y Responsables de los Sistemas afectados.

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, sin perjuicio de la posibilidad de delegar esta tarea.

e) Asegurarse de que los permisos necesarios para el acceso a los diferentes aplicativos informáticos correspondientes al personal que ya no tenga que acceder al servicio prestado, se revoquen o deshabiliten en los sistemas relacionados.

Artículo 22. ***Los Puntos o Personas de Contacto (POC)***

De conformidad con lo previsto en el artículo 13.5 del Esquema Nacional de Seguridad, 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 23. ***Función Diferenciada***

De conformidad con lo previsto en el artículo 13.3 del Esquema Nacional de Seguridad, 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 Esquema Nacional de Seguridad.

Artículo 24. ***Clasificación y control de activos en materia de Seguridad TIC***

1. Los recursos informáticos y la información de la Consejería en base al Esquema Nacional de Seguridad se encontrarán inventariados. Este inventario contará con la persona responsable de seguridad TIC de la Consejería, que será la 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 25. ***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 Esquema Nacional de Seguridad, la facultad para efectuar las valoraciones a las que se refiere su artículo 40, 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.

Artículo 26. ***Auditorías de la seguridad en materia de Seguridad TIC.***

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

2. Los informes de auditoría serán presentados a la persona responsable del sistema competente, al Delegado o Delegada de Protección de Datos, si afectara a estos, y a la persona responsable de la Unidad de Seguridad TIC. Estos informes serán analizados por esta última persona que presentará sus conclusiones a la persona Responsable del Sistema para que adopte las medidas correctoras adecuadas. Los resultados obtenidos determinarán las líneas de actuación a seguir y las posibles modificaciones a realizar sobre los controles y la normativa de seguridad.

3. Con el fin de optimizar la utilización de los recursos públicos y garantizar una mejor coordinación entre seguridad TIC y seguridad de protección de datos, siempre que sea posible, las auditorías de seguridad de sistemas de información y las auditorías de protección de datos o medidas análogas de verificación, evaluación y valoración de seguridad de los tratamientos se realizarán de manera conjunta.

CAPÍTULO IV
Política de Seguridad Interior

Artículo 27. ***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 28. ***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 ejercerá 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. Las funciones de la Unidad de Seguridad Interior, en el ámbito de la Consejería, conforme a lo previsto en el artículo 10.2 Decreto 171/2020, de 13 de octubre, serán las siguientes:

a) Realizar las labores de soporte, asesoramiento e información al Comité de Seguridad, así como la ejecución de sus decisiones y acuerdos en materia de seguridad interior y la propuesta de un Plan de Seguridad Interior para esta Consejería.

b) Proponer las adaptaciones necesarias al ámbito de la seguridad interior, incluso valores, tablas y métricas adecuadas al conjunto de los activos en su ámbito.

c) Realizar el desarrollo, el mantenimiento y la supervisión del marco regulador de la seguridad interior en esta Consejería.

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

e) Recoger de forma sistemática información y supervisar el estado de las principales variables de seguridad interior en el ámbito de esta Consejería.

f) Realizar la coordinación y el seguimiento de la actividad de los puntos coordinadores responsables de seguridad interior de esta Consejería e cada provincia.

g) Realizar el asesoramiento técnico y la auditoría del sistema de seguridad interior en el ámbito de esta Consejería.

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

i) Gestionar para el ámbito de esta 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 esta Consejería.

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

l) Asegurar en el ámbito de esta 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, conforme a la normativa vigente en materia de protección de datos personales.

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

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

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

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

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

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 de Coordinación previstos en el artículo 30, así como con los distintos responsables que en esta materia se establezcan en las Delegaciones Territoriales de la Consejería.

Artículo 29. *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 30. *Puntos Coordinadores de Seguridad Interior*

1. A nivel provincial existirán Puntos Coordinadores de Seguridad Interior que serán asumidos por personal de las Delegaciones Territoriales de la Consejería designados al efecto por el Comité de Seguridad Interior y Seguridad TIC 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 31. ***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 32. ***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.

Artículo 33. Auditorías de la seguridad en materia de seguridad interior.

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

CAPÍTULO V
Política de protección de datos personales

Artículo 34. ***Ámbito de aplicación y marco normativo***

1. La política de protección de datos personales de la Consejería será aplicable a todos los tratamientos de datos personales realizados por sus órganos en el ejercicio de las competencias que tengan atribuidas. Asimismo, será de aplicación a las actividades de tratamiento que dichos órganos efectúen por cuenta de otros responsables del tratamiento, en calidad de encargados

2. Esta política de protección de datos personales de la Consejería se aplicará en el marco de lo dispuesto en el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en la Ley Orgánica 3/2018, de 5 de diciembre, y, cuando resulte aplicable, en la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales

3. En dicho ámbito, cada responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas para garantizar y poder demostrar que los tratamientos de datos personales se realizan conforme a la normativa aplicable, de acuerdo con el principio de responsabilidad proactiva, conforme a lo previsto en el artículo 5.2 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en el artículo 28 de la Ley Orgánica 3/2018, de 5 de diciembre, y en el artículo 6.5 de la Ley Orgánica 7/2021, de 26 de mayo".

Artículo 35. ***Delegado o Delegada de Protección de Datos***

1. La Consejería y cada una de sus entidades vinculadas o dependientes contará con una persona que ostente la condición de Delegado o Delegada de Protección de Datos, a efectos de lo

establecido en los artículos 37 a 39 del Reglamento General de Protección de Datos (RGPD), en los artículos 34 a 37 de la Ley Orgánica 3/2018, de 5 de diciembre y, cuando sean de aplicación, los artículos 40 a 42 de la Ley Orgánica 7/2021, de 26 de mayo.

2. El Delegado o la Delegada de Protección de Datos de la Consejería será nombrada por la persona responsable del tratamiento en los supuestos previstos en el artículo 37.1 del Reglamento General de Protección de Datos, atendiendo a las cualidades profesionales, conocimientos y capacidad establecidos en el artículo 37.5 del mismo cuerpo normativo, y estará adscrito a ese órgano directivo. En el nombramiento deberá especificarse el alcance de su designación, indicando los responsables de tratamiento para los que ejercerá sus funciones, que podrá alcanzar a una o varias de las entidades vinculadas o dependientes de la Consejería.

En las entidades vinculadas o dependientes de la Consejería, el Delegado o Delegada de Protección de Datos será designada por la persona que asuma la dirección de la entidad correspondiente.

En todo caso, el Delegado o Delegada de Protección de Datos de la Consejería colaborará y se coordinará con las entidades vinculadas o dependientes de la misma en todas las cuestiones relativas a su ámbito de competencia, estableciendo mecanismos de colaboración con las personas responsables de protección de datos de dichas entidades.

La designación, nombramiento y cese del Delegado o Delegada de Protección de Datos de la Consejería será notificada al Consejo de Transparencia y Protección de Datos de Andalucía, conforme a lo establecido en el Reglamento General de Protección de Datos y en el artículo 34.3 de la Ley Orgánica 3/2018, de 5 de diciembre.

3. De conformidad con lo dispuesto en en el Reglamento General de Protección de Datos y en la Ley Orgánica 3/2018, de 5 de diciembre, el Delegado o la Delegada de Protección de Datos de la Consejería, en el ejercicio de sus funciones, actuará con plena independencia, debiendo evitarse cualquier conflicto de intereses. No podrá ser removido ni sancionado por el desempeño de sus funciones, salvo que hubiese incurrido en dolo o negligencia grave en su ejercicio. En el ejercicio de sus funciones tendrá acceso a los datos personales y procesos de tratamiento sin que las personas responsables o encargadas puedan oponer la existencia del deber de confidencialidad, incluso el previsto en el artículo 5 de la Ley Orgánica 3/2018, de 5 de diciembre.

4. El Delegado o Delegada de Protección de Datos podrá poner en conocimiento del Comité de Seguridad Interior y Seguridad TIC las cuestiones relacionadas con la protección de datos que considere necesarias.

5. Son funciones de la persona que ostente la condición de Delegado o Delegada 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, 38 y 39.1 del Reglamento General de Protección de Datos, en los artículos 36.1 y 36.4 , 37 y 65.4 de la Ley Orgánica 3/2018, de 5 de diciembre, y, en su caso, en los artículos 41. 1 41.4 y 42 de la Ley Orgánica 7/2021, de 26 de mayo, que son las siguientes:

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

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

c) Asesorar a la persona responsable del tratamiento al realizar la evaluación de impacto relativa a la protección de datos, tanto en la necesidad de su realización como en su elaboración y en la necesidad o no de consulta previa a la autoridad de control, y supervisar su aplicación.

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

e) Participar de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales.

f) Actuar como interlocutor del responsable o encargado del tratamiento ante la Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos.

g) Documentar y comunicar inmediatamente a los órganos de administración y dirección del responsable o el encargado del tratamiento la existencia de una vulneración relevante en materia de protección de datos.

h) Intervenir en caso de reclamación ante las Autoridades de Protección de Datos.

i) Mantener sus conocimientos especializados, contando con los recursos necesarios para el desempeño de sus funciones y acceso a los datos personales y a las operaciones de tratamiento.

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.

2. En el caso de los órganos directivos periféricos de la Consejería, los Responsables de los Tratamientos serán las Delegaciones Territoriales, 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, teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, de conformidad con el artículo 24.1 del Reglamento general 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 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 un contrato o acto jurídico con arreglo al Derecho de la Unión Europea o de los Estados miembros de la misma, incluido el ordenamiento jurídico español, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable y las estipulaciones previstas en el artículo 28.3 del Reglamento General de Protección de Datos y demás normativa de aplicación. 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. Dichas estipulaciones se incluirán, al menos, en los siguientes actos jurídicos:

a) Todos los contratos que impliquen tratamiento de datos , incluidos los menores.

b) Encargos a medios propios.

c) Encomiendas de gestión.

d) Convenios que impliquen encargo de tratamiento de datos.

e) Subvenciones que impliquen encargo de tratamiento de datos

4. 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. *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. Esto es, información relativa a:

a) El nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos.

b) Los fines del tratamiento

c) Una descripción de las categorías de interesados y de las categorías de datos personales

d) Las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;

e) En su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49.1, párrafo segundo, del Reglamento de protección de datos, la documentación de garantías adecuadas.

f) Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos.

g) Si es posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 32.1 del Reglamento General de Protección de Datos.

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 responsable del tratamiento aprobará mediante resolución la creación, actualización, modificación y exclusión del registro de las actividades de tratamiento de datos personales de dicho órgano, comunicándolo a la persona que ostente la condición de Delegado o Delegada de Protección de Datos, conforme a lo estipulado en el artículo 31.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

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, accesible a través de la sección de transparencia del portal de la Junta de Andalucía, 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 y con el artículo 31.2 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

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

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

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

1. Conforme al principio de protección de datos personales desde el diseño, al que se refiere el artículo 25.1 del Reglamento General de Protección de Datos, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias, a fin de cumplir los requisitos de dicho Reglamento y proteger los derechos de las personas interesadas.

2. Conforme al principio de protección de datos personales por defecto del artículo 25.2 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 en el procedimiento de elaboración de disposiciones generales desde el diseño, el órgano directivo proponente incorporará, en la Memoria de Análisis de Impacto Normativo (MAIN), una evaluación de impacto en la protección de datos personales. Esta evaluación será puesta en conocimiento de la persona que ostente la condición de Delegado o Delegada de Protección de Datos por parte de la unidad administrativa u órgano que lleve a cabo la tramitación del procedimiento, y contendrá, al menos, referencia a:

a) Si la aprobación del proyecto requiere un alta, baja o modificación de actividades de tratamiento en el Registro de Actividades de Tratamiento.

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

c) Si la aprobación del proyecto supone 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.

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. Cuando exista duda sobre la incidencia de un anteproyecto de ley o proyecto de disposición general en materia de protección de datos, podrá recabarse con carácter previo el criterio de la persona que ostente la condición de Delegado o Delegada de Protección de Datos, a fin de determinar la procedencia de solicitar dicho 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 41. ***Seguridad de tratamientos automatizados***

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 (RGPD), 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 42. *Seguridad de tratamientos no automatizados*

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

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

1. Al objeto de determinar las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con la normativa de protección de datos, el responsable realizará, 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 44. ***Evaluación de Impacto en la Protección de Datos (EIPD)***

1. Cuando sea probable que un tipo de tratamiento de datos personales, 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 45.1 de la presente orden. Para ello, recabará el asesoramiento de la persona que ostente la condición de Delegado de Protección de Datos. La realización de la evaluación de impacto se requerirá en particular en los supuestos contemplados en el artículo 35.3 del Reglamento General de Protección de Datos así como en los casos en que sea necesaria conforme a las listas que publique la autoridad de control.

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

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

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

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

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

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

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

Artículo 45. ***Violaciones de la Seguridad de los Datos Personales***

1. Se aprobará un protocolo de gestión de posibles violaciones de la seguridad de los datos personales, de conformidad con los artículos 33 y 34 del Reglamento General de Protección de Datos (RGPD) 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 la 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 de los datos. La documentación 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, de conformidad con el artículo 33.1 del Reglamento General de Protección de Datos.

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, de conformidad con el artículo 34 del Reglamento General de Protección de Datos (RGPD). La comunicación al interesado describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 33, apartado 3, letras b), c) y d) del mencionado Reglamento.

Artículo 46. ***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 47. ***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 los 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 deberán incorporar cualquier aspecto que sea necesario o aconsejable desde el punto de vista de la normativa en materia de protección de datos.

Artículo 48. ***Comunicaciones oficiales con la autoridad de control***

1. La persona titular del órgano responsable del tratamiento suscribirá los siguientes documentos y comunicaciones relacionados con las potestades del Consejo de 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 vulneraciones en 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 o Delegada de Protección de Datos.

Disposición adicional primera. ***Constitución del Comité de Seguridad Interior y Seguridad TIC.***

1. La primera convocatoria del Comité de Seguridad tendrá por objeto la constitución del mismo y se celebrará en un plazo máximo de seis meses a partir de la entrada en vigor de la presente Orden. Durante la celebración de la sesión constitutiva se procederá a realizar las designaciones que competen a este órgano según lo dispuesto en la presente Orden.

2. Asimismo, en la sesión constitutiva del Comité de Seguridad y para aquella información, servicios y sistemas que se encuentren inventariados, se verificarán las designaciones de los Responsables de la Información, del Servicio y del Sistema.

Disposición adicional segunda. ***Deber de colaboración en la implementación de la Política de Seguridad de la Consejería*****.**

Los órganos y unidades de la Consejería deberán colaborar en las actuaciones de implementación de las políticas de seguridad interior, seguridad TIC y protección de datos personales.

Disposición adicional tercera. ***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 derogatoria única. ***Derogación normativa***

Queda derogada, en cuanto al ámbito sectorial competencial asumido por la Consejería de Turismo y Andalucía Exterior, la Orden de 15 de noviembre de 2023, por la que se establece la política de seguridad de la Consejería de Turismo, Cultura y Deporte en los ámbitos de seguridad interior, seguridad de las tecnologías de la información y comunicaciones y de la protección de

datos personales, así como cuantas disposiciones de igual o inferior rango se opongan a lo establecido en la presente Orden.

Disposición final primera. ***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.

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.

Sevilla, a ** de ** de 2025

Carlos Arturo Bernal Bergua
Consejero de Turismo y Andalucía Exterior