3. Otras disposiciones

CONSEJERÍA DE AGRICULTURA, PESCA, AGUA Y DESARROLLO RURAL

Orden de 5 de noviembre de 2024, por la que se establece la política de seguridad de la información de la Consejería de Agricultura, Pesca, Agua y Desarrollo Rural.

P R E Á M B U L O

El Decreto del Presidente 6/2024, de 29 de julio, sobre reestructuración de Consejerías, establece la organización en Consejerías de la Administración de la Junta de Andalucía y mantiene para la Consejería de Agricultura, Pesca, Agua y Desarrollo Rural (en adelante la Consejería), las competencias que tenía ya atribuidas, así como las hasta ahora ejercidas por la Consejería de Sostenibilidad, Medio Ambiente y Economía Azul en materia de uso, gestión y conservación sostenible de los recursos marinos y por la Consejería de la Presidencia, Interior, Diálogo Social y Simplificación Administrativa en materia de protección y tenencia de los animales de compañía. El Decreto 157/2022, de 9 de agosto, modificado por el Decreto 165/2024, de 26 de agosto, establece la estructura orgánica de la Consejería y las funciones que corresponden a sus órganos directivos en aras de la mejor gestión de las competencias asignadas.

En el ámbito de actuación de la Consejería, los avances tecnológicos de la informática, las telecomunicaciones y de la sociedad de la información son ya un hecho consolidado, que afecta no solo a la sociedad sino también a la Consejería como poder público. Son los poderes públicos los responsables de generar confianza en el uso por parte de la ciudadanía de los medios tecnológicos en sus relaciones con la Administración Pública y confianza en el uso seguro que realiza ésta de la información que registra, almacena y procesa. Para conseguir esta confianza, permitiendo tanto a la ciudadanía, los profesionales y las empresas, como a las Administraciones Públicas, el ejercicio de derechos y el cumplimiento de deberes, los medios tecnológicos utilizados deben ser seguros y para ello se debe garantizar la confidencialidad, integridad y disponibilidad de la información, de los sistemas, de las comunicaciones y de los servicios telemáticos, al igual que la vigilancia, protección de las personas, órganos, edificios, establecimientos y dependencias propias de la Consejería, como garantía de funcionamiento de nuestras instalaciones y de la seguridad de los personas usuarias de nuestros servicios.

Las Leyes 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, vienen a configurar un escenario en el que la tramitación electrónica debe constituir la actuación habitual de las Administraciones en sus múltiples vertientes de gestión interna, de relación con la ciudadanía y de relación de aquellas entre sí.

En concreto, la Ley 39/2015, de 1 de octubre, tiene como uno de sus objetivos centrales regular las relaciones entre las Administraciones y la ciudadanía y empresas, teniendo en cuenta el desarrollo de las tecnologías de la información y comunicación de los últimos años y cómo este afecta a las relaciones entre estos agentes. Pretende implantar una Administración totalmente electrónica, interconectada y transparente, mejorando la agilidad de los procedimientos administrativos y reduciendo los tiempos de tramitación. Por su parte, la Ley 40/2015, de 1 de octubre, procura dotar a nuestro sistema legal de una norma comprensiva del régimen jurídico de las Administraciones Públicas, regulando el funcionamiento interno de cada Administración y de las relaciones entre ellas.

00310779

El Estatuto de Autonomía para Andalucía, en su artículo 34, reconoce el derecho a acceder y usar las nuevas tecnologías y a participar activamente en la sociedad del conocimiento, la información y la comunicación, mediante los medios y recursos que la ley establezca. Asimismo, el artículo 58.1.2.º atribuye a la Comunidad Autónoma de Andalucía competencias exclusivas sobre el régimen de las nuevas tecnologías relacionadas con la Sociedad de la Información y del Conocimiento, en el marco de la legislación del Estado.

Por otro lado, la Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía, señala en su artículo 7.2 que los principios que rigen las relaciones que mantenga la Administración de la Junta de Andalucía con la ciudadanía y con otras Administraciones Públicas a través de redes abiertas de telecomunicación son los de simplificación y agilización de trámites, libre acceso, accesibilidad universal y confidencialidad en el tratamiento de la información, y de seguridad y autenticidad en orden a la identificación de las partes y el objeto de la comunicación. Para ello establece que estos sistemas deben cumplir con el requisito de existencia de medidas de seguridad que eviten la interceptación y alteración de las comunicaciones, así como los accesos no autorizados. En este mismo texto legal se abunda en materia de seguridad señalándose que los medios o soportes en que se almacenen los documentos electrónicos contarán con las medidas de seguridad que garanticen la integridad, protección y conservación de los documentos almacenados, así como la identificación de las personas usuarias y el control de acceso de los mismos.

Para el desarrollo de esta Política de seguridad de la información de la Consejería, se ha seguido lo dispuesto en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, 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 y su modificación mediante el Decreto 70/2017, de 6 de junio, y la Orden 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.

Adicionalmente, se tienen en cuenta en esta Política de Seguridad los aspectos de seguridad digital requeridos por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos) y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Igualmente se ha atendido a lo dispuesto en el Decreto 171/2020, de 13 de octubre, por el que se establece la Política de Seguridad Interior en la Administración de la Junta de Andalucía contra riesgos intencionales y que integra en un único Comité a las personas responsables de la Seguridad Interior de los activos de cada Consejería con las personas responsables de la Seguridad TIC.

Se han tenido también en cuenta los preceptos requeridos por la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas y de su correspondiente Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas, al ser la Consejería operador de este tipo de infraestructuras.

Igualmente, se tiene en cuenta lo establecido por el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, así como 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.

Se contempla también que la Consejería, en su calidad de Organismo Pagador de Fondos Europeos, está obligada a implantar un sistema de gestión de seguridad de la

00310779

información en base a lo dispuesto en el Anexo I, apartado 3.B del Reglamento Delegado (UE) núm. 2022/127 de la Comisión, de 7 de diciembre de 2021, que completa el Reglamento (UE) 2021/2116 del Parlamento Europeo y del Consejo con normas relativas a los organismos pagadores y otros órganos, la gestión financiera, la liquidación de cuentas, las garantías y el uso del euro. Adicionalmente, se tiene en cuenta el establecimiento de un Perfil de Cumplimiento Específico del ENS para Organismos Pagadores por parte del Centro Criptológico Nacional en su Guía CCN-STIC 852 «Aplicación del ENS en Organismos Pagadores».

Se contempla además la creación de la Agencia Digital de Andalucía, mediante la disposición adicional vigesimosegunda de la Ley 3/2020, de 28 de diciembre, del Presupuesto de la Comunidad Autónoma de Andalucía para el año 2021, teniendo como fines la definición y ejecución de los instrumentos de tecnologías de la información, telecomunicaciones, ciberseguridad y gobierno abierto y su estrategia digital en el ámbito de la Administración General, Administración educativa y de Justicia. Adicionalmente, se contempla la categorización de la Agencia como encargado de tratamiento de datos personales cuando en el ejercicio de sus funciones trate datos cuya responsabilidad recae en la Consejería, de acuerdo a la Disposición Adicional Cuarta del Decreto 128/2021, de 30 de marzo, por el que se aprueban los Estatutos de la Agencia Digital de Andalucía.

También se atiende a lo establecido en el «Código de Conducta en el uso de las Tecnologías de la Información y la Comunicación para profesionales públicos de la Administración de la Junta de Andalucía*, aprobado por Resolución de 22 de octubre de 2020, de la Secretaría General para la Administración Pública.

Esta política de seguridad de la información establece el compromiso de la Consejería con la seguridad integral de sus activos, define los objetivos y criterios básicos para el tratamiento de la misma, sienta los pilares del marco normativo de seguridad en este organismo y la estructura organizativa y de gestión que velará por su cumplimiento, utilizando el concepto de información como eje vertebrador que pone en valor a los diferentes tipos de activos (personas, dependencias, infraestructuras, sistemas de información, equipamiento TIC...) que permiten su gestión.

Por otra parte, de acuerdo con el artículo 5 de la Ley 12/2007, de 26 de noviembre, para la promoción de la igualdad de género en Andalucía, esta norma integra el principio de igualdad de género de forma transversal en su elaboración, garantizando con ello un impacto positivo en la igualdad de oportunidades entre mujeres y hombres.

En la elaboración y tramitación de la presente orden, se ha actuado conforme a los principios de buena regulación a los que se refiere el artículo 129.1 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. En cuanto a los principios de necesidad y eficacia, la orden no hace sino cumplir con los mandatos de los ya citados 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 su modificación mediante el Decreto 70/2017, de 6 de junio, y Decreto 171/2020, de 13 de octubre, por el que se establece la Política de Seguridad Interior en la Administración de la Junta de Andalucía contra riesgos intencionales; cumple con el de proporcionalidad al desarrollar estrictamente el mandato de dichos decretos, no imponiendo más obligaciones a la ciudadanía ni a la Administración que los establecidos en éstos y regulando las figuras necesarias para el cumplimiento de la finalidad perseguida; sobre el de seguridad jurídica, se han tenido en cuenta todas las normas europeas, estatales y autonómicas de aplicación; acerca del de transparencia, al tratarse de una disposición de organización interna no ha habido consulta previa ni trámite de audiencia a la ciudadanía, limitándose los informes a los internos de la Administración; y, es eficiente porque no solo evita imponer cargas administrativas adicionales, sino que se limita a utilizar los recursos ya existentes para prestar los servicios requeridos sin que suponga ningún incremento de gasto.

00310779

En su virtud, a propuesta de la Secretaria General Técnica, conforme a lo establecido en el Decreto 157/2022, de 9 de agosto, por el que se establece la estructura orgánica de la Consejería, modificado por el Decreto 165/2024, de 26 de agosto, y en uso de las facultades que me confiere el artículo 44.2 de la Ley 6/2006, de 24 de octubre, del Gobierno de la Comunidad Autónoma de Andalucía,

D I S P O N G O

CAPÍTULO I

Disposiciones generales

Artículo 1. Objeto.

1. La presente orden tiene por objeto establecer la política de seguridad de la información (en adelante PSI), en el ámbito de la Consejería de Agricultura, Pesca, Agua y Desarrollo Rural (en adelante Consejería), así como su marco organizativo y tecnológico. El alcance de la PSI engloba cualquier aspecto específico relativo a la política de seguridad de las tecnologías de la información y comunicaciones (en adelante TIC), a la política de seguridad interior y a la política de seguridad de datos personales.

2. La presente orden constituye el documento de política de seguridad de la información de la Consejería.

Artículo 2. Misión de la Consejería.

1. La misión de la Consejería se corresponde con la propuesta y ejecución de las directrices del Gobierno de Andalucía en relación con las competencias que les son atribuidas en el artículo 1 del Decreto 157/2022, de 9 de agosto, por el que se establece la estructura orgánica de la Consejería, modificado por el Decreto 165/2024, de 26 de agosto.

Artículo 3. Ámbito de aplicación.

1. La política de seguridad de la información de la Consejería será de aplicación además de a sus órganos directivos centrales y periféricos, a las entidades vinculadas o dependientes de la misma en cada momento, en coordinación con lo establecido en las posibles políticas de seguridad propias de estas y otras dependencias derivadas de posibles dobles adscripciones de entidades.

2. Deberá ser observada por todo el personal que acceda a sus sistemas de información o a la propia información que sea gestionada por la Consejería, mediante el uso de activos de tecnologías de la información y comunicaciones o de cualquier otro tipo, con independencia de cuál sea su destino, adscripción o relación con la misma.

Artículo 4. Marco normativo.

1. Se asume como marco normativo general el que en cada momento aplique a la Consejería en virtud de su naturaleza legal y sus competencias.

2. Se asume como marco normativo específico en seguridad TIC el que sea definido en cada momento por la Consejería u organismo competente en este ámbito. Se asume como marco normativo específico en seguridad interior el que sea definido en cada momento por la Consejería u organismo competente en este ámbito.

3. La normativa aplicable en los ámbitos anteriormente mencionados deberá estar recogida en un listado de requisitos legales aplicables, disponible para su consulta y que tendrá que mantenerse actualizado.

4. La Consejería podrá ampliar y desarrollar su marco documental específico en materia de seguridad de la información en los términos previstos en el artículo 22 de esta orden.

00310779

CAPÍTULO II

Política de seguridad de la información

Artículo 5. Objetivos de la política de seguridad de la información.

1. Son objetivos de la política de seguridad de la información de la Consejería:

a) Garantizar la seguridad de la información, protegiendo los activos o recursos de información.

b) Crear la estructura básica de organización de la seguridad de la información de la Consejería, así como los mecanismos para su posible ampliación.

c) Marcar las directrices, los objetivos y los principios básicos de seguridad de la información de la organización.

d) Orientar la organización hacia la prestación de servicios basados en la gestión de riesgos, a través de un único modelo integral de gestión de la seguridad de la información, que cubra un ciclo continuo de mejora.

e) Servir de base para el desarrollo de las normas, procedimientos y procesos de gestión de la seguridad de la información.

2. Estos objetivos incorporan para el ámbito de actuación de la Consejería los objetivos establecidos para la Administración de la Junta de Andalucía y contenidos en el artículo 4 del Decreto 1/2011, de 11 de enero, relativos a la política de seguridad de las tecnologías de la información y comunicaciones, y en el artículo 4 del Decreto 171/2020, de 13 de octubre, por el que se establece la Política de Seguridad Interior en la Administración de la Junta de Andalucía contra riesgos intencionales, relativos a la política de seguridad interior.

Artículo 6. Principios básicos de la seguridad de la información.

1. Los principios básicos que regirán la política de seguridad de la información de la Consejería serán los establecidos en el Esquema Nacional de Seguridad (en adelante ENS) por el artículo 5 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, en la Política de Seguridad TIC de la Junta de Andalucía, en el artículo 5 del Decreto 1/2011, de 11 de enero, y por la Política de seguridad interior en la Administración de la Junta de Andalucía, en el artículo 5 del Decreto 171/2020, de 13 de octubre, integrándose en los siguientes:

a) Gestión integral de la seguridad: la seguridad se definirá y gestionará como un proceso integral constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con los sistemas de información de la Consejería, sobre los que se procurará el mantenimiento de sus dimensiones de confidencialidad, autenticidad, integridad, disponibilidad, trazabilidad y privacidad. Se prestará especial atención a la concienciación de los diferentes intervinientes en el proceso y sus superiores jerárquicos, con objeto de favorecer la necesaria coordinación imprescindible para minimizar los riesgos en la seguridad.

b) Gestión de la seguridad basada en riesgos: todos los sistemas incluidos en el alcance de esta política deberán estar incluidos en un análisis de riesgos que se realizará al menos anualmente, siguiendo una metodología reconocida, identificando y valorando los activos, evaluando las amenazas y las salvaguardas aplicadas. Se elaborará un informe del análisis de riesgos realizado y un plan de mejora de la seguridad de la información para el tratamiento de dichos riesgos que revalúe la idoneidad de las medidas de seguridad existentes y las actualice cuando sea necesario, de acuerdo con el principio de proporcionalidad en costes económicos y operativos y con el principio de prioridad en la protección de las personas en relación a los activos.

Este análisis se revisará al menos cuando cambie la información manejada o los servicios prestados, cuando ocurra un incidente grave de seguridad o se reporten vulnerabilidades críticas.

c) Prevención, detección, respuesta y conservación. Se deben implementar las medidas 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

00310779

y riesgos. Estos controles estarán claramente definidos y documentados, en orden a reducir la posible materialización de amenazas, favorecer su rápida detección y permitir una eficaz gestión de la respuesta y restauración de la información y servicios afectados.

Se adoptarán medidas que permitan detectar incidentes de seguridad y se establecerán canales adecuados para su comunicación y mecanismos para responder eficazmente a los incidentes en el menor tiempo posible, 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.

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, así como la conservación de los datos e información en soporte electrónico.

d) Existencia de líneas de defensa. Se adoptará una estrategia de protección basada en múltiples capas de seguridad, constituidas por medidas organizativas, físicas y lógicas, que permitan evitar en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad y desarrollar una adecuada reacción ante los mismos, evitando una afectación del conjunto de activos.

e) Principio de vigilancia continua y re-evaluación periódica. 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 revisión de alertas, eventos y logs 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.

f) Principio de responsabilidad. Todas las personas que de una forma u otra participen en la utilización, operación, administración o gestión de un sistema de información, serán responsables de observar las normas de seguridad establecidas. Para ello las correspondientes responsabilidades deberán quedar determinadas de forma explícita, y ser comunicadas a cada una de ellas.

Se diferenciará el responsable de la información, el responsable del servicio, el responsable de la seguridad y el responsable del sistema, estando diferenciada la responsabilidad sobre la explotación de los sistemas de información respecto a la responsabilidad de la seguridad.

g) Gestión de la seguridad en el ciclo de vida de los activos: los recursos informáticos y la información se encontrarán inventariados, con una persona responsable asociada y, en caso de ser necesario, una persona custodia de los mismos. Los inventarios se mantendrán actualizados para asegurar su validez. Los activos de información estarán clasificados de acuerdo a su sensibilidad y criticidad para el desarrollo de la actividad de la Consejería, en función de la cual se establecerán las medidas de seguridad exigidas para su protección, teniéndose en cuenta las especificaciones de seguridad en todas las fases del ciclo de vida de los mismos.

Artículo 7. Requisitos mínimos de seguridad.

La política de seguridad de la información de la Consejería se desarrollará de acuerdo a los siguientes requisitos mínimos, exigibles en proporción a los riesgos identificados para cada sistema:

a) Organización e implantación del proceso de seguridad, que debe comprometer a todo el personal de la Consejería, informados y conocedores de la presente política y de las responsabilidades de su cumplimiento.

b) Análisis y gestión de los riesgos.

c) Gestión de personal. Se implantarán los mecanismos necesarios para que cualquier persona que acceda o pueda acceder a los sistemas de información de la Consejería

00310779

conozca sus responsabilidades, y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos.

d) Profesionalidad. La seguridad de los sistemas de información estará atendida, revisada y auditada por personal cualificado.

e) Autorización y control de los accesos. Se limitará el acceso a los activos de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes con su calificación y sujetos a plazos de vigencia.

f) Protección de las instalaciones. Los sistemas de información estarán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su criticidad. Los locales donde se ubiquen los sistemas dispondrán de elementos adecuados para el eficaz funcionamiento del equipamiento allí instalado.

g) Adquisición de productos de seguridad y contratación de servicios de seguridad. Las diferentes unidades organizativas identificarán los requisitos de seguridad a incluir para la adquisición de productos o la contratación de servicios.

h) Seguridad por defecto. Con anterioridad a la puesta en servicio de cualquier sistema de información será obligatorio verificar que cumple los requisitos y especificaciones de seguridad que se hubieran establecido.

i) Integridad y actualización del sistema. Se requerirá una autorización formal previa a la instalación de un sistema por parte del responsable del servicio. Se deberá conocer el estado de la seguridad del sistema en relación con las recomendaciones y actualizaciones de seguridad recomendadas por el fabricante.

j) Protección de la información almacenada y en tránsito. Toda la información almacenada de forma centralizada será periódicamente respaldada. La información que se transmita a través de redes de comunicaciones o soportes portátiles estará adecuadamente protegida, teniendo en cuenta su calificación y criticidad, mediante mecanismos que garanticen su seguridad.

k) Prevención ante otros sistemas de información interconectados. Se dispondrá de sistemas de protección del perímetro de los sistemas de la Consejería, permitiendo únicamente el tránsito de los flujos previamente autorizados. Se asegurará la autenticidad del otro extremo de un canal de comunicación antes de intercambiar información alguna.

l) Registro de actividad. Se registrarán aquellos eventos que se consideren de interés, tanto para la detección de actividades que puedan comprometer la seguridad, como para dejar constancia de aquellas otras actividades que permitan verificar y evidenciar la efectividad de los controles, las normas de seguridad establecidas por la Consejería y los requisitos legales aplicables.

m) Incidentes de seguridad, ante los que se dispondrá de un adecuado procedimiento de gestión.

n) Continuidad de la actividad. Las unidades organizativas deberán elaborar planes de continuidad del negocio. Se implantarán mecanismos apropiados para asegurar la disponibilidad de los sistemas de información teniendo en cuenta la valoración de la dimensión de disponibilidad.

ñ) Mejora continua del proceso de seguridad, aplicando criterios y métodos reconocidos en la práctica nacional e internacional.

Artículo 8. Estructura organizativa de la seguridad de la información.

1. La gestión de la seguridad de la información va íntimamente ligada al establecimiento de una organización de seguridad. Dicha organización se establece mediante la identificación de las diferentes actividades y responsabilidades en materia de gestión de la seguridad y mediante su asignación formal a los agentes que correspondan, agrupadas en los siguientes bloques de responsabilidad:

a) La especificación de las necesidades y requisitos en materia de seguridad de la información.

b) El desarrollo y/o explotación de sistemas de información.

00310779

c) La función de supervisión de la seguridad de los sistemas de información y de la seguridad interior.

2. La estructura organizativa básica de gestión de la seguridad de la información en el ámbito de la Consejería estará compuesta por los siguientes agentes:

a) Comité de Seguridad de la Información.
b) Unidad de Seguridad de la Información.
c) Unidad de Seguridad Interior y Puntos Coordinadores de Seguridad Interior.
d) Personas responsables de la Información.
e) Personas responsables de los Servicios.
f) Personas responsables de los Sistemas.
g) Persona responsable de Seguridad y Enlace de Infraestructuras Críticas.
h) Responsable de Seguridad de la Información de Servicios Esenciales.
i) Delegado/a de Protección de Datos.
j) Responsables o encargados de tratamientos de datos personales.

3. En cada una de las entidades vinculadas o dependientes existirá una estructura organizativa de gestión de la seguridad de la información que estará compuesta al menos por:

a) Comité de Seguridad Interior y de Seguridad TIC.
b) Personas responsables de la Información.
c) Personas responsables de los Servicios.
d) Personas responsables de los Sistemas.
e) Persona responsable de Seguridad.
f) Unidad de Seguridad Interior y Puntos Coordinadores de Seguridad Interior, si el Comité los considera necesarios por virtud del volumen o singularidad de los activos de la entidad.
g) Delegado/a de Protección de Datos.
h) Responsables o encargados de tratamientos de datos personales.

4. Dependiendo de las necesidades y circunstancias de la organización, en ciertos casos, la función de algunos de estos agentes podrá recaer sobre una misma persona, unidad o departamento, teniendo en cuenta las siguientes salvedades:

a) De acuerdo con el artículo 11.2 del Real Decreto 311/2022, de 3 de mayo, y artículo 5.j) del Decreto 1/2011, de 11 de enero, la responsabilidad de la seguridad de los sistemas de tecnologías de la información y comunicaciones estará diferenciada de la responsabilidad sobre la prestación de los servicios, no pudiendo recaer en una misma persona la condición de responsable de seguridad y la de responsable de la información, servicios o sistemas.

b) Las que se deriven de la normativa reguladora en materia de Infraestructuras Críticas, Servicios Esenciales, Protección de Datos Personales y, en particular. la posible existencia de conflicto de intereses.

c) De conformidad con la organización interna de la Consejería, las responsabilidades que esta orden asocie a las personas titulares de los centros directivos serán incompatibles con las de responsable de sistemas, de seguridad o de delegado/a de protección de datos.

5. Este modelo organizativo tiene el carácter de mínimo, pudiendo la Consejería o sus entidades vinculadas o dependientes crear subcomités o perfiles adicionales con responsabilidad en seguridad, para una mejor consecución de los objetivos y principios establecidos en esta Política mediante la ejecución de las funciones que se le puedan encomendar. Las propuestas de nuevas estructuras o perfiles de seguridad deberán ser remitidas, para su estudio y aprobación, al Comité de Seguridad de la Información, especificando las funciones que se le asignarán y, en caso de perfiles, las competencias requeridas para su desempeño.

6. Con sujeción al marco previsto por el ENS, por la normativa en materia de protección de datos, por la políticas de seguridad TIC y de seguridad interior de la Junta de Andalucía y por sus normativas de desarrollo, en las entidades vinculadas o dependientes de la Consejería la responsabilidad de la conformación y designación de estas figuras, recaerá sobre las propias entidades vinculadas o dependientes.

00310779

Artículo 9. Comité de Seguridad de la Información de la Consejería.

1. Se crea el Comité de Seguridad de la Información de la Consejería, que no tiene carácter colegiado para la dirección y seguimiento en materia de seguridad de los activos físicos y de información de los que la Consejería sea titular o cuya gestión tenga encomendada. Estará adscrito al órgano directivo de la Consejería que ostente las competencias en materia de Seguridad de la Información.

2. El Comité de Seguridad de la Información de la Consejería estará formado por los siguientes miembros:

a) La persona titular del órgano directivo de la Consejería que ostente las competencias en materia de Seguridad de la Información, que ejercerá la presidencia del Comité; la cual tendrá voto de calidad en la toma de decisiones del Comité en caso de empate.

b) La persona titular de la Coordinación del órgano directivo de la Consejería que ostente las competencias en materia de Seguridad de la Información, que ejercerá la vicepresidencia del Comité.

c) La persona titular de cada uno de los Centros Directivos de la Consejería con rango de Viceconsejería o un representante, de nivel 28 o superior, por designación de la anterior, que actuará como vocal.

d) La persona titular del órgano directivo de la Consejería al que corresponda la dirección del Organismo Pagador de Andalucía de Fondos Europeos Agrarios o un representante, de nivel 28 o superior, por designación de la anterior, que actuará como vocal.

e) La persona designada por la Agencia Digital de Andalucía, de nivel 28 o superior, como responsable del soporte que proporciona a la Consejería en materia de Tecnologías de la Información y Comunicaciones, que actuará como vocal.

f) Dos representantes, por designación de la persona titular de la Secretaría General Técnica, seleccionados entre las personas que ostenten las jefaturas de los Servicios de la Secretaría General Técnica con competencias en Legislación, Contratación, Personal y Administración General, que actuarán como vocales.

g) La persona que hubiere sido designada Delegado/a de Protección de Datos, que actuará como vocal, con voz pero sin voto.

h) La persona que hubiere sido designada Responsable de Seguridad y Enlace de las infraestructuras críticas responsabilidad de la Consejería, que actuará como vocal.

i) La persona que hubiere sido designada Responsable de Seguridad de la Información de los servicios de información de la Consejería categorizados como esenciales, que actuará como vocal. Si dicha designación hubiese recaído en un unidad u órgano colegiado, actuará como vocal la persona titular de la unidad o una persona designada por la presidencia del órgano colegiado.

j) La persona titular de la Unidad de Seguridad Interior, que actuará como vocal.

k) La persona titular de la Unidad de Seguridad de la Información, que actuará como vocal y que ejercerá la secretaría del Comité; podrá delegar esta función en un técnico/a de su Unidad, que asistiría a las reuniones del Comité con voz pero sin voto.

3. Se habilita el siguiente esquema de suplencias para el caso de que las personas titulares no puedan acudir a las reuniones del mismo.

a) Los vocales titulares de centros directivos podrán ser sustituidos por las personas titulares de las correspondientes Coordinaciones. Los vocales que ostenten la Coordinación de un órgano directivo podrán ser sustituidos por la persona que designe de su propio órgano de nivel 28 o superior.

b) Las personas titulares de centros directivos que designen vocales, deberán igualmente proponer sus posibles sustitutos.

c) Los restantes miembros podrán designar a una persona suplente que asuma sus funciones interinamente por ausencia o enfermedad; en caso de vacante, la designación se hará por la persona titular de la presidencia. Se procurará que la persona suplente pertenezca al mismo órgano directivo que la persona vocal a la que suple y deberá contar además con similar cualificación y requisitos establecidos para el cargo.

00310779

4. En las designaciones de vocales y suplentes del Comité de Seguridad de la Información se procurará tener en cuenta la composición de género que permita la representación equilibrada de mujeres y hombres.

5. Serán funciones propias del Comité de Seguridad de la Información en el ámbito de la Consejería y sus entidades vinculadas o dependientes:

a) Impulsar el conocimiento y cumplimiento de la política de seguridad de la información y su desarrollo normativo, estableciendo las directrices comunes y de supervisión de seguridad de la información.

b) Aprobar las propuestas de creación de nuevas estructuras o perfiles de seguridad y ofrecer asesoramiento, de ser requerido, respecto al nombramiento de perfiles de seguridad.

c) Realizar tareas de coordinación con los Comités de Seguridad Interior y Seguridad TIC de las entidades instrumentales vinculadas o dependientes de la Consejería.

d) Velar por la coordinación entre los diferentes planes estratégicos en materia de seguridad de la información que puedan coexistir tanto en la Consejería como en sus entidades vinculadas o dependientes.

e) Informar regularmente a la persona titular de la Consejería del estado de la seguridad de la información en su ámbito.

f) Elevación de propuestas de revisión de la política de seguridad de la información de la Consejería, de directrices y normas de seguridad de la Consejería, o de revisión de los marcos normativos de seguridad interior y de seguridad TIC de la Junta de Andalucía, a los órganos competentes para su reglamentaria tramitación.

6. Serán funciones propias del Comité de Seguridad de la Información en el ámbito de la Consejería:

a) Impulsar el conocimiento y cumplimiento de la política de seguridad de la información y su desarrollo normativo, estableciendo las directrices comunes y de supervisión de seguridad de la información.

b) Definir, aprobar y realizar el seguimiento de los objetivos, iniciativas y planes estratégicos en materia de seguridad de la información.

c) Promover la implantación y mejora continua del sistema de gestión de la seguridad de la información (en adelante SGSI) de la Consejería.

d) Velar por la disponibilidad de los recursos necesarios para desarrollar las iniciativas y planes estratégicos definidos y priorizar las actuaciones en materia de seguridad en la Consejería.

e) Designar la Unidad de Seguridad de la Información de la Consejería entre las unidades existentes en la misma o ratificar la propuesta de cobertura de esta Unidad realizada por la Agencia Digital de Andalucía, de entre sus propias unidades y previa solicitud del Comité, garantizándose siempre el principio de función diferenciada.

f) Designar la Unidad de Seguridad Interior de la Consejería.

g) Designar a las personas responsables de los sistemas, o ratificar la propuesta de designación realizada por la Agencia Digital de Andalucía previa solicitud del Comité.

h) Dirimir cualquier posible conflicto respecto a la asignación de responsabilidades sobre la información y los servicios.

i) Establecer las normas básicas de funcionamiento del Grupo de Respuesta ante Incidentes de Seguridad de la Información y, en su caso, designar entre sus miembros a participantes en el mismo, adicionales a la composición mínima establecida en esta Política.

j) Identificación de la normativa aplicables a la Consejería en el ámbito de la Seguridad de la Información, manteniendo actualizado y aprobando el listado de requisitos legales aplicables.

k) Determinar los niveles de calificación de la información gestionada por la Consejería, estableciendo y documentando los criterios de aplicación.

l) Aprobación de los documentos del SGSI de la Consejería correspondientes al segundo y tercer nivel de los definidos en el artículo 22 de esta Política.

00310779

m) Coordinar los esfuerzos de todo el equipo humano con responsabilidad en materia de seguridad, elevando propuesta para la resolución de los conflictos de competencia que se puedan suscitar entre ellos, o resolviéndolos cuando el superior jerárquico de los mismos no pueda hacerlo o delegue su resolución.

n) Promoción de formación, entrenamiento y concienciación sobre las medidas legales y organizativas relativas a la seguridad de la información entre el personal de la Consejería, aprobando los planes anuales de formación.

o) Coordinar y aprobar los planes de continuidad de la Consejería.

p) 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.

q) Supervisar el nivel de riesgo y la toma de decisiones en la respuesta a incidentes de seguridad que afecten a los activos de información, monitorizando el desempeño de los procesos de gestión de incidentes de seguridad.

r) Impulsar la determinación de los niveles de seguridad de la información tratada, en la que se valorarán los impactos que tendrían los incidentes que afectaran a la seguridad de la información, todo ello con la participación de las personas Responsables de la Información correspondientes y de la Unidad de Seguridad de la Información.

s) Impulsar los preceptivos análisis de riesgos, junto a las personas Responsables de la Información y de los Servicios que correspondan, contando con la participación de la Unidad de Seguridad de la Información.

t) Establecer el nivel de riesgo aceptable, por encima del cual deberían adoptarse medidas enfocadas a la reducción del riesgo de las amenazas identificadas, y la aprobación de los planes de tratamiento que se definan a este respecto.

u) Coordinar la aceptación de los riesgos residuales por sus responsables correspondientes respecto de la información y/o servicios de su competencia, obtenidos en el análisis de riesgos.

v) Coordinar las medidas técnicas y organizativas establecidas para el cumplimiento de la normativa de protección de datos personales, de acuerdo con los correspondientes análisis de riesgos y, en su caso, las evaluaciones de impacto en la protección de datos, contando con el asesoramiento de la persona delegada de protección de datos.

Artículo 10. Funcionamiento del Comité.

1. El Comité se reunirá con carácter ordinario al menos dos veces al año y, con carácter extraordinario cuando lo decida la persona titular de la presidencia, de oficio o a propuesta de alguno de sus miembros, y siempre que se produzcan incidencias de seguridad graves o surjan nuevas necesidades de seguridad que requieran la participación del Comité.

2. El Comité podrá constituirse, convocar y celebrar sus sesiones, adoptar acuerdos y remitir actas, tanto de forma presencial como a distancia, utilizando redes de comunicación, 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. Para su válida constitución y a todos los efectos, se requerirá la asistencia de la presidencia y la secretaría del Comité o en su caso, de quienes les suplan, y la de la mitad, al menos de sus miembros; los acuerdos serán adoptados por mayoría de votos, teniendo la presidencia voto dirimente en caso de empate.

3. Cuando el tratamiento de determinadas cuestiones lo requiera, se podrá convocar a las reuniones del Comité a personal técnico especializado, a los efectos de prestar asesoramiento experto, sin que en ningún caso pueda ocasionar coste económico.

4. La persona que ostente la secretaría del Comité levantará acta de cada reunión del mismo, pudiendo estar soportada ésta en documentación y evidencias electrónicas generadas en el desarrollo de la reunión, que deberán conservarse de forma que se garantice su integridad y autenticidad y la posibilidad de acceso a los mismos por parte de los miembros del Comité.

00310779

Las personas miembros del Comité de Seguridad y cualquier asistente a sus reuniones están obligadas a respetar la confidencialidad de toda la información a la que tengan acceso.

5. El Comité de Seguridad de la Información establecerá entre sus miembros un grupo de respuesta a incidentes de seguridad de la información, cuya función será la toma urgente de decisiones en caso de contingencia grave que afecte a la seguridad de los activos o sistemas de información críticos de la Consejería.

Sus normas básicas de funcionamiento, que pueden ser ampliadas por el propio Comité, son las siguientes:

- El grupo será convocado a reunión, presencial o a distancia, por el Presidente del Comité, ante la sospecha de la existencia de tales contingencias.
- Las decisiones se adoptarán por mayoría simple de sus miembros, tras la exposición y discusión de las circunstancias existentes, disponiendo el Presidente del Comité voto dirimente en caso de empate.
- Las decisiones serán comunicadas al personal y órganos directivos afectados a la mayor urgencia posible, por el miembro del grupo que reciba ese encargo, en función de su ámbito habitual de competencias.
- Las decisiones adoptadas por este grupo serán sometidas con prontitud al conocimiento del Comité y a la revisión posterior de su eficacia por éste, quedando documentadas por la persona que ejerza la secretaría del Comité.

La composición mínima inicial de este grupo, que puede ser ampliada por el propio Comité, es la siguiente:

- Persona titular de la presidencia del Comité de Seguridad de la Información.
- Persona responsable de la Unidad de Seguridad de la Información de la Consejería.
- Persona responsable de la Unidad de Seguridad Interior de la Consejería.
- Persona o personas responsables de los Sistemas.
- Delegado/a de Protección de Datos, realizando funciones de asesoría

Artículo 11. Unidad de seguridad de la Información.

1. Es la unidad administrativa que asume la responsabilidad de que los servicios y sistemas de información se mantengan con el mayor grado de seguridad, atendiendo a los principios establecidos en esta Política y supervisando el SGSI implantado. Esta unidad tendrá las atribuciones en materia de seguridad TIC que establece el artículo 11.1 del Decreto 1/2011, de 11 de enero.

2. La Unidad de Seguridad de la Información de la Consejería será nombrada o renovada, en caso de tratarse de una unidad administrativa perteneciente a la Consejería, o ratificada, en caso de unidad administrativa externa propuesta por el organismo con competencias en esta materia, por el Comité de Seguridad de la Información, mediante acto documentado que se comunicará a la persona responsable que se encuentre a su frente. Esta designación deberá garantizar el cumplimiento del principio de función diferenciada recogido en el artículo 11 del Esquema Nacional de Seguridad y en el artículo 5.j) del Decreto 1/2011, de 11 de enero.

3. Sus funciones dentro del ámbito de la Consejería son:

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

b) Supervisar el cumplimiento de la presente Política, y de sus normas y procedimientos derivados.

c) Asesorar en materia de seguridad de la información a los integrantes de la Consejería que así lo requieran.

d) Coordinación en materia de seguridad de la información en la Consejería y con otros organismos especializados.

e) Tomar conocimiento y supervisar la investigación y monitorización de los incidentes de seguridad.

00310779

f) Categorizar los diferentes sistemas de información existentes en el ámbito de la Consejería y establecer las medidas de seguridad adecuadas y eficaces para cumplir los requisitos de seguridad definidos por las personas Responsables de los Servicios y de la Información afectados por el ENS, siguiendo en todo momento lo exigido en el Anexo II del ENS (Medidas de Seguridad).

g) Establecer las medidas de seguridad adecuadas y eficaces para cumplir los requisitos de protección de datos personales, siguiendo en todo momento lo dispuesto en la normativa de Protección de Datos Personales y contando con el asesoramiento del delegado/a de protección de datos.

h) Trasladar los requisitos y medidas de seguridad a aplicar durante el desarrollo de la actividad a las personas Responsables de sistemas, velando por su cumplimiento, para lo que deberá establecer directrices que posibiliten su demostración.

i) Desarrollo y seguimiento de programas de formación y concienciación en su ámbito de competencia.

j) Asesorar y participar en el proceso de la gestión de los riesgos a realizar por las personas Responsables de la Información, de los Servicios o de los Sistemas, en relación con la adquisición, incorporación, desarrollo o modificación de productos o sistemas de información o en el desarrollo de nuevos proyectos.

k) Elaborar el análisis de riesgos de la Consejería y elevar un informe anual sobre el estado del proceso de gestión de riesgos al Comité de Seguridad de la Información.

l) Promover y realizar el seguimiento de las auditorías periódicas que den cumplimiento a las obligaciones en materia de seguridad de la información.

m) Analizar los informes de auditoría, presentando las conclusiones al Comité de Seguridad de la Información, transmitiendo con posterioridad los resultados a las diferentes personas responsables para que adopten las medidas correctoras oportunas.

n) Elaborar informes periódicos de seguridad para el Comité de Seguridad de la Información, con inclusión y estudio de los incidentes más relevantes de cada período y la gestión realizada de los mismos, así como de los principales riesgos residuales asumidos por la organización, recomendando posibles actuaciones respecto de ellos.

4. Tendrá la condición de Responsable de Seguridad la persona responsable de la Unidad de Seguridad de la Información, o la designada desde ella para el ejercicio de estas funciones, y en virtud del artículo 10.4 del Decreto 1/2011, de 11 de enero, la presente política establece que le corresponderán los deberes y responsabilidades correspondientes en los términos recogidos en el ENS y la guía CCN-STIC-801.

5. La Unidad de Seguridad de la Información de la Consejería elaborará y mantendrá un inventario de servicios y sistemas, con indicación expresa de su categorización según el ENS y las personas u órganos que asumen, para cada uno de ellos, las figuras de responsable de la información, responsable del servicio y responsable del sistema. Dicho listado se entregará, actualizado, al Comité de Seguridad TIC del organismo en cada una de sus reuniones, con indicación de aquellas deficiencias o faltas de información que se produzcan, de modo que el Comité disponga de información completa y pueda arbitrar los mecanismos necesarios para la subsanación de las mismas.

Artículo 12. Unidad de seguridad interior y Puntos coordinadores de seguridad interior.

1. La Unidad de seguridad interior es la unidad administrativa de la Consejería que asume la responsabilidad ejecutiva para la seguridad interior del conjunto de los activos en su ámbito, atendiendo a los principios establecidos en esta Política. Esta unidad tendrá las atribuciones y funciones que establece el artículo 10 del Decreto 171/2020, de 13 de octubre.

2. La Unidad de Seguridad interior de la Consejería será nombrada o renovada por el Comité de Seguridad de la Información, mediante acto documentado que se comunicará a la persona responsable que se encuentre a su frente.

00310779

3. Los Puntos coordinadores de seguridad interior tendrán las atribuciones y funciones que establece el artículo 13 del Decreto 171/2020, de 13 de octubre. Serán nombrados por la persona titular del órgano directivo con competencias en materia de seguridad interior.

Artículo 13. Personas responsables de la información y de los servicios de la Consejería

1. Las personas Responsables de la información y/o de los servicios serán las personas titulares de los centros directivos que decidan sobre la finalidad, contenido y uso de la información y/o sobre las características de los servicios a prestar, así como las que determinen los niveles de seguridad dentro del marco establecido en el Anexo I del ENS.

2. En virtud del artículo 10.4 del Decreto 1/2011, de 11 de enero, los deberes y responsabilidades principales de estos perfiles de responsabilidad, dentro de su ámbito de actuación y sin perjuicio de otras previstas en el ENS y la guía CCN-STIC-801, son los siguientes:

a) Determinar los requisitos de seguridad de la información y/o de los servicios a prestar, identificando los niveles de seguridad de la información y/o servicios mediante la valoración del impacto sobre los mismos de los incidentes que pudieran producirse.

b) Determinar el nivel de calificación que debe aplicarse a la información bajo su responsabilidad y promover el correcto etiquetado de sus posibles soportes.

c) Proporcionar la información necesaria a la Unidad de Seguridad de la Información para realizar los preceptivos análisis de riesgos, con la finalidad de establecer las salvaguardas a implantar. Para ello contará con la ayuda de la persona Responsable del Sistema (o las personas Responsables si hubiere varias).

d) En relación con los análisis de riesgos de los sistemas de información, aceptar los riesgos residuales de las informaciones manejadas y/o servicios prestados que sean de su competencia.

3. El nombramiento o renovación de estas figuras responsables se realiza en virtud de la presente política de seguridad de la información, estando aparejados automáticamente a la toma de posesión de la titularidad de los correspondientes centros directivos o unidades organizativas y a la adscripción a los mismos en cada momento de las distintas informaciones manejadas y servicios prestados.

Artículo 14. Personas responsables de los sistemas.

1. La figura de Responsable del sistema, desde la perspectiva del ENS, de cada sistema de información que gestione la Consejería, deberá ser asignada a la persona titular de un Servicio, o cargo equivalente, con competencias en Tecnologías de la Información y Comunicaciones, de la Consejería o del organismo de la Junta de Andalucía que le preste soporte TIC.

2. La asignación de dicha responsabilidad se realizará por decisión del Comité de Seguridad de la Información de la Consejería y se comunicará, mediante acto documentado, a la persona o personas designadas.

3. En el caso de aquellos sistemas de información cuya implantación, explotación y mantenimiento se haga fuera de la Consejería, mediante empresa externa, ésta deberá asumir la responsabilidad de esta figura, debiendo formalizarse a través de los correspondientes acuerdos y contratos, de los que deberá ser informado el Comité de Seguridad de la Información de la Consejería.

4. En virtud del artículo 10.4 del Decreto 1/2011, de 11 de enero, la presente política establece que los deberes y responsabilidades de este perfil de responsabilidad serán los previstos en el ENS y la guía CCN-STIC-801 para la figura del Responsable del Sistema.

Artículo 15. Persona responsable de Seguridad y Enlace de Infraestructuras Críticas.

1. La Consejería tiene la consideración de Operador de Infraestructuras Críticas, por lo que se encuentra obligada a la designación de una persona Responsable de Seguridad

00310779

y Enlace con la Administración y a su comunicación formal a la autoridad competente, en base a lo dispuesto en el artículo 16.1 de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

2. La persona Responsable de Seguridad y Enlace velará en el marco organizativo de la Consejería por la garantía de la seguridad de la información relativa a las infraestructuras críticas y a sus planes de protección, según la clasificación de la información almacenada.

3. Deberá ser informado y participar en el análisis y tratamiento de cualquier incidente de seguridad que afecte a la información y sistemas relativos a infraestructuras críticas, debiendo velar por su correcta resolución.

4. Los sistemas, las comunicaciones y la información referida a la protección de las infraestructuras críticas contarán con las medidas de seguridad necesarias que garanticen su confidencialidad, integridad y disponibilidad, según el nivel de clasificación que les sea asignado.

5. El Comité de Seguridad de la Información actuará como punto de coordinación respecto de otros posibles Operadores de Infraestructuras Críticas en el caso de que las mismas se localicen físicamente en instalaciones de la Consejería.

Artículo 16. Responsable de Seguridad de la Información de Servicios Esenciales.

1. La Consejería puede tener la consideración de Operador de Servicios Esenciales, por lo que se encontraría obligada a la designación del Responsable de Seguridad de la Información de los Servicios Esenciales y su comunicación formal a la autoridad competente, respecto a la que actuará como punto de contacto y de coordinación técnica, en base a lo dispuesto en el artículo 16.3 del Real Decreto-Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

2. El Responsable de Seguridad de la Información de Servicios Esenciales velará en el marco organizativo de seguridad de la Consejería por la adopción de medidas técnicas y de organización, adecuadas y proporcionadas, para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información utilizados en la prestación de los servicios esenciales por parte de la Consejería, así como la notificación de incidentes y la adopción de medidas adecuadas para prevenir y reducir al mínimo el impacto de los incidente les afecten.

3. El rol de responsable de Seguridad de la Información de Servicios Esenciales puede ser desempeñado por una persona, unidad u órgano colegiado.

Artículo 17. Delegado/a de Protección de Datos.

1. La figura del Delegado/a de Protección de Datos, en los términos establecidos en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos, en adelante RGPD), podrá ser asumida por una persona o grupo de personas de la Consejería, en base a la existencia de una plaza específica en la Relación de Puestos de Trabajo o por simple asignación de funciones, o por una persona externa, física o jurídica. En cualquiera de estos casos, se deberá acreditar a nivel personal conocimientos especializados en derecho y competencia en materia de protección de datos. Tendrá una adscripción dentro de la estructura de la organización a un órgano con competencias y funciones de carácter horizontal, a los efectos de poder relacionarse adecuadamente con la dirección de la organización y con las autoridades de control, contando con plena independencia de actuación en el ejercicio de sus funciones.

2. En los casos en que la figura esté atribuida a un grupo de personas de la Consejería, una de ellas ostentará la responsabilidad de su coordinación, convocará sus reuniones y ejercerá la función de su representación, quedando este hecho explícitamente recogido en el acto de nombramiento. Este grupo de trabajo podrá celebrar sus reuniones y adoptar acuerdos, tanto de forma presencial como a distancia, utilizando redes de comunicación,

00310779

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. Los acuerdos serán adoptados por mayoría de votos, teniendo la persona coordinadora del grupo voto dirimente en caso de empate.

3. El nombramiento o cese de la figura del Delegado/a de Protección de Datos se realizará y comunicará, mediante acto documentado, por la persona titular de la Viceconsejería, con el parecer, si es requerido, del Comité de Seguridad de la Información de la Consejería. En el nombramiento deberá especificarse el alcance de su designación, indicando los responsables de tratamiento para los que ejercerá sus funciones. El nombramiento o cese de la figura del Delegado/a de Protección de Datos se comunicará a la autoridad de control correspondiente de acuerdo con el artículo 34.3 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

4. El Delegado/a de Protección de Datos deberá desempeñar las funciones y responsabilidades asignadas a dicha figura por la normativa en materia de protección de datos recogida en el artículo 22 de esta orden.

5. El Delegado/a de Protección de Datos de la Consejería velará por la elaboración y mantenimiento de un registro unificado de tratamientos de datos personales, para lo que contarán con la colaboración de los responsables del tratamiento. En dicho registro constará indicación expresa de las personas u órganos que asumen las figuras de responsable del tratamiento, encargado del tratamiento y resto de requisitos exigidos por el artículo 30 del RGPD y por el artículo. 31 de la Ley Orgánica 3/2018, de 5 de diciembre (LOPDGDD). Dicho listado se entregará actualizado al Comité de Seguridad de la Información de la Consejería en sus reuniones en caso de que haya sido modificado. Asimismo deberá informar de posibles deficiencias o faltas de información que se produzcan, de modo que el Comité pueda arbitrar los mecanismos necesarios para la subsanación de las mismas.

Artículo 18. Responsables y encargados de tratamientos de datos personales.

1. Los Responsables de los Tratamientos de datos personales de la Consejería serán los órganos directivos que determinen los fines y medios de los tratamientos, de conformidad con el artículo 4.7 del RGPD.

2. Los órganos directivos que realicen tratamientos de datos personales cuya responsabilidad resida en un tercero tendrán la consideración de encargado de tratamiento de conformidad con el artículo 4.8 del RGPD.

3. Los centros directivos, responsables o encargados de tratamientos, deberán desempeñar las funciones y responsabilidades asignadas a dichas figuras por la normativa en materia de protección de datos recogida en el articulo 23 de esta orden.

Artículo 19. Resolución de conflictos.

1. En caso de conflicto entre diferentes personas, unidades u órganos responsables, éste será resuelto por el órgano superior jerárquico de los mismos. En defecto de lo anterior, prevalecerá la decisión del Comité de Seguridad de la Información.

2. En los conflictos entre las personas responsables que componen la estructura organizativa de la política de seguridad de la información de la Consejería y las personas responsables definidas en virtud de la normativa de protección de datos personales prevalecerá la decisión que presente un mayor nivel de exigencia respecto a la protección de los datos personales. En caso de conflicto en la determinación de dicho nivel de exigencia, prevalecerá la decisión del Comité de Seguridad de la Información.

3. En caso de conflicto de atribuciones se actuará de acuerdo a lo previsto en el artículo 110 de la Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía.

00310779

Artículo 20. Responsabilidad del Personal.

1. La preservación de la seguridad de la información será considerada objetivo común de todas las personas al servicio de los órganos contemplados en el ámbito de aplicación de esta norma, siendo éstas responsables del uso correcto de los activos, de información y/o tecnológicos, puestos a su disposición.

2. Todas las personas que presten servicios a la Consejería tienen la obligación de conocer y cumplir, en sus respectivos ámbitos de actuación, la presente política de seguridad, así como la normativa de seguridad que emana de la misma, siendo responsabilidad del Comité de Seguridad de la Consejería facilitar los medios necesarios para que la información llegue a los interesados.

3. El incumplimiento manifiesto de la Política de Seguridad de la Información o la normativa y procedimientos derivados de ésta podrá acarrear el inicio de las oportunas medidas disciplinarias y, en su caso, las responsabilidades legales correspondientes.

4. Con carácter general, para el personal de la Consejería, regirán las normas de comportamiento de los empleados públicos en el uso de los sistemas informáticos y redes de comunicaciones de la Administración de la Junta de Andalucía vigentes en cada momento.

5. Las normas de uso de los recursos derivadas de esta Política serán trasladadas convenientemente, en la medida en que pueda resultar necesario o recomendable, al clausulado de los contratos suscritos por la Consejería.

Artículo 21. Terceras partes.

1. Cuando la Consejería preste servicios a otros organismos o maneje información de estos, se les hará partícipes de esta política de seguridad de la información, estableciéndose los canales que procedan para la comunicación y coordinación entre las respectivas organizaciones, en especial para una rápida y eficaz reacción ante incidentes de seguridad.

2. Cuando la Consejería utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta política de seguridad de la Información y de la normativa de seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta, a través de cláusulas contractuales o acuerdos de nivel de servicio, a las obligaciones generales establecidas en dicha normativa y, específicamente, a la obligación de comunicar incidentes de seguridad que puedan afectar la seguridad de los sistemas o información de la Consejería, pudiendo disponer la tercera parte de sus propios procedimientos operativos para satisfacerlas. Se establecerán mecanismos de comunicación y resolución de incidencias. Se velará por que el personal de terceros esté adecuadamente concienciado en materia de seguridad, al menos, al mismo nivel que el establecido en esta política de seguridad de la información.

3. Cuando algún aspecto de esta política de seguridad de la información no pueda ser satisfecho por una tercera parte según se requiere en el párrafo anterior, se requerirá un informe de la Unidad de Seguridad de la Información que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá que, antes de continuar con las actuaciones, las personas responsables de la información y/o los servicios afectados asuman expresa y plenamente el informe.

Artículo 22. Desarrollo documental de la seguridad de la información.

1. El conjunto de documentos que integran el SGSI se desarrollará en cinco niveles, según el ámbito de aplicación y nivel de detalle técnico requerido, de manera que cada documento de un determinado nivel se fundamente en los documentos del nivel superior. Dichos niveles de desarrollo documental son los siguientes:

a) Primer nivel: Política de Seguridad de la Información. Documento de obligado cumplimiento por todo el personal de la Consejería, aprobado por la persona titular de la Consejería.

b) Segundo nivel: Normativas de seguridad, que desarrollan y detallan la Política de Seguridad de la Información, estableciendo premisas que deben cumplir las personas

00310779

usuarias en un área o aspecto determinado. Son documentos de carácter horizontal y de obligado cumplimiento para todo el personal de la Consejería en sus respectivos ámbitos de actuación; serán aprobadas por el Comité de Seguridad de la Información.

c) Tercer nivel: Procedimientos de seguridad, que detallan las anteriores normativas de seguridad especificando sus procesos de realización. Son documentos de obligado cumplimiento de acuerdo al ámbito organizativo, técnico o legal correspondiente. Los procedimientos se aprobarán por el Comité de Seguridad de la Información; en su redacción podrán participar las unidades organizativas que participen en el proceso normalizado con la supervisión de la Unidad de Seguridad de la Información.

d) Cuarto nivel: Instrucciones Técnicas de Seguridad de la información, documentos muy detallados a nivel técnico, orientados a pautar determinadas tareas, consideradas críticas por el perjuicio que causaría una actuación inadecuada en las mismas. Su aprobación recae en la persona responsable del área donde se desarrollen las actividades descritas en cada instrucción.

e) Quinto nivel: Informes, registros y otras evidencias, documentación que permite probar el cumplimiento de requisitos y la puesta en práctica de los procedimientos e instrucciones establecidos en los niveles anteriores. La responsabilidad de su generación es de las personas responsables de las áreas donde se desarrollen cada una de las actividades.

2. Al amparo de la presente orden, la Consejería podrá ampliar y desarrollar, sobre la base de los mínimos establecidos, sus propias normas en materia de seguridad TIC, en virtud del artículo 2.5 de la Orden 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.

3. Además de los documentos citados en el apartado 1, la documentación de seguridad de la información de los órganos contemplados en el ámbito de aplicación de esta norma podrá contar, bajo criterio de la Unidad de Seguridad de la Información con otros documentos de carácter no vinculante: recomendaciones, buenas prácticas, etc.

4. La Unidad de Seguridad de la Información deberá mantener la documentación de seguridad actualizada y organizada, y gestionar los mecanismos de acceso a la misma, de conformidad con las normas y procedimientos de gestión que se establezcan.

5. El Comité de Seguridad de la Información establecerá los mecanismos necesarios para compartir la documentación derivada del desarrollo documental con el propósito de normalizarlo, en la medida de lo posible, en todo el ámbito de aplicación de la Política.

Artículo 23. Seguridad de los Datos Personales.

1. Para el tratamiento de datos personales por parte de la Consejería se seguirá en todo momento lo establecido en el RGPD, en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y en la restante legislación europea, nacional y autonómica vigente en cada momento en relación con esta materia. En aplicación del principio de responsabilidad proactiva establecido en el RGPD, la Consejería debe ser capaz de demostrar la conformidad de los tratamientos de datos realizados con dicha normativa.

2. La gestión de la seguridad de los datos personales se basará en implantación de medidas técnicas y organizativas desde el diseño y por defecto, con vistas a la reducción del riesgo asociado a la tipología y volumen de los mismos y a la naturaleza de los tratamientos efectuados.

Artículo 24. Gestión de riesgos.

1. La gestión de riesgos debe realizarse de manera continua sobre los activos de información e infraestructuras de la Consejería, conforme a los principios de gestión de la seguridad basada en los riesgos y de re-evaluación periódica.

00310779

2. El proceso de gestión de riesgos comprende las fases de identificación y valoración de la información manejada y de los servicios prestados, categorización de los sistemas, análisis de riesgos y selección de medidas de seguridad a aplicar, las cuales deberán ser proporcionales a los riesgos y estar justificadas.

3. Este análisis de riesgos deberá realizarse por parte de la Unidad de Seguridad de la información, a partir de la información proporcionada y con la participación de las personas responsables de servicios, de la información y de los sistemas, al menos de forma anual o cuando se produzcan cambios importantes en la información manejada o los servicios prestados o ante vulnerabilidades e incidentes de seguridad graves. Como resultado, se elevará el correspondiente informe al Comité de Seguridad de la información, para el establecimiento del nivel de riesgo aceptable y, cuando proceda, la propuesta de medidas a aplicar para evitar los riesgos identificados, así como de planes de tratamiento pertinentes.

4. Las personas responsables de la información y/o servicios son responsables de los riesgos sobre su información y/o servicios y, por tanto, de aceptar los riesgos residuales calculados en el análisis de riesgos, así como de realizar su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.

5. En los supuestos de sistemas de información que traten datos personales, el responsable o el encargado del tratamiento, asesorado por la figura del delegado/a de protección de datos, realizará un análisis de riesgos teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento conforme al artículo 24 del RGPD y, en los supuestos de su artículo 35, una evaluación de impacto en la protección de datos. Los responsables del tratamiento, serán responsables de aplicar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.

6. El Comité de Seguridad de la información realizará un seguimiento de los riesgos y de la eficacia de las medidas adoptadas para su tratamiento.

7. Para la realización de análisis de riesgos se utilizarán metodologías y herramientas reconocidas en el ámbito de la Administración Pública.

Artículo 25. Prevención, detección y respuesta frente a incidentes de seguridad y continuidad de los servicios.

1. La Consejería deberá estar preparado para prevenir, detectar, reaccionar y recuperarse de incidentes, según los términos previstos en los artículos 8 y 25 del ENS.

2. El Comité de Seguridad de la Información deberá aprobar y revisar periódicamente un plan para mantener la continuidad de los procesos y sistemas críticos y garantizar su recuperación en caso de desastre. La finalidad de este plan es reducir el tiempo de indisponibilidad a niveles aceptables mediante la combinación de controles de carácter organizativo, tecnológico y procedimental tanto preventivos como de recuperación.

3. A los efectos de una mejor gestión de los incidentes, se actuará de forma coordinada con el Centro de Respuesta a Incidentes de Seguridad de la Junta de Andalucía.

Artículo 26. Formación y concienciación en seguridad de la información.

El Comité de Seguridad de la Información aprobará un Plan anual de formación y concienciación en seguridad de la información que, salvaguardando las competencias específicas de los organismos corporativos con funciones en este ámbito, contemplará las actividades necesarias, destinadas a las personas contempladas en el ámbito de aplicación de esta política, para fomentar la conciencia de seguridad integral, sensibilizada respecto a los riesgos de seguridad que afectan a todo el personal y en todas sus actividades de tratamiento de la información. Entre tales actividades se incluirán las de difusión de esta política de seguridad y de su desarrollo normativo.

Artículo 27. Auditorías y conformidad con la normativa.

1. La Consejería realizará revisiones periódicas independientes sobre su SGSI, establecido para implementar esta Política de Seguridad, con objeto de garantizar el

00310779

cumplimiento normativo vigente y su adecuación respecto a estándares internacionales de seguridad.

2. Los sistemas de información de la Consejería serán objeto, al menos cada dos años, de una auditoría regular ordinaria interna y externa que verifique el cumplimiento de los requisitos del ENS. Independientemente, se realizarán aquellas auditorías que sean requeridas por otras normas o estándares que apliquen o se implanten en la Consejería. La Unidad de Seguridad de la Información realizará o, en su caso, coordinará, estas actividades de auditoría.

3. El sistema de seguridad interior de la Consejería será objeto de una auditoría regular ordinaria interna o externa que verifique su funcionamiento respecto de las normas o estándares que apliquen o se implanten en la Consejería. La Unidad de Seguridad Interior realizará o, en su caso, coordinará, estas actividades de auditoría.

4. Con carácter extraordinario deberán realizarse dichas auditorías siempre que se realicen modificaciones sustanciales en el SGSI, en los sistemas de información y, en general, en los activos de la Consejería, que puedan repercutir en el cumplimiento de las medidas de seguridad requeridas.

5. Los informes de auditoría quedarán a disposición del Comité de Seguridad de la Información. Por su parte, la Unidad de Seguridad de la Información y la Unidad de Seguridad Interior deberán analizar cada informe y elevar al Comité de Seguridad de la Información las conclusiones que procedan para que éste adopte las medidas correctoras adecuadas.

6. La Consejería auditará su cumplimiento de la normativa de protección de datos de forma periódica, al menos cada dos años. La persona con funciones de Delegado de Protección de Datos realizará o, en su caso, coordinará, estas actividades de auditoría, trasladando el informe de auditoría y sus conclusiones a la Dirección de la Consejería, así como a los responsables del tratamiento, a fin de que adopten las medidas correctivas necesarias.

Artículo 28. Cooperación con otros órganos y otras administraciones en materia de seguridad de la información.

A efectos de coordinación, obtención de asesoramiento e intercambio de experiencias para la mejora continua de la gestión de la seguridad de la información, se fomentará el establecimiento de mecanismos de comunicación por parte de los agentes definidos en el artículo 8 de esta orden con otros agentes especializados en esta materia, en base a sus respectivas funciones y ámbitos de actuación. En especial, se contemplarán los siguientes:

- El Comité de Seguridad TIC de la Junta de Andalucía y el Comité Corporativo de Seguridad Interior de la Junta de Andalucía.
- La Unidad de Seguridad TIC de la Junta de Andalucía y la Unidad Corporativa de Seguridad Interior.
- La Agencia Digital de Andalucía.
- El Centro de Ciberseguridad de Andalucía y su Centro de Operaciones de Seguridad (SOC).
- El Centro de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional (CCN), como soporte y coordinación para la resolución de incidentes que sufran las administraciones públicas.
- El Instituto Nacional de Ciberseguridad.
- El Grupo de Delitos Telemáticos de la Guardia Civil y la Brigada de Investigación Tecnológica del Cuerpo Nacional de Policía, para la investigación de acciones relacionadas con la delincuencia informática y los fraudes en el sector de las telecomunicaciones.
- La Agencia Española de Protección de Datos y el Consejo de Transparencia y Protección de Datos de Andalucía.

00310779

Artículo 29. Revisión, actualización permanente y difusión de la Política de Seguridad de la Información.

1. La política de seguridad de la información deberá mantenerse actualizada para adecuarla a la evolución tecnológica y al desarrollo de la sociedad de la información, así como a los estándares internacionales de seguridad.

2. Las revisiones de la política de seguridad de la información se harán al menos con carácter anual por el Comité de Seguridad de la información, proponiendo su revisión o el mantenimiento de la misma. Las modificaciones en la política de seguridad serán aprobadas por la persona titular de la Consejería.

3. A los efectos de su mejor difusión entre el personal de la organización y de otras partes interesadas, la política de seguridad de la información se publicará y divulgará, además de en el Boletín Oficial de la Junta de Andalucía, a través de los medios que se establezcan por el Comité de Seguridad de la Información.

Disposición adicional única. Constitución del Comité de Seguridad de la Información.

La primera reunión del Comité de Seguridad de la Información tendrá por objeto la constitución del mismo y se celebrará en un plazo máximo de un mes a partir de la entrada en vigor de la presente orden. En dicha reunión se procederá a la designación o confirmación de la Unidad de Seguridad de la Información y de la Unidad de Seguridad Interior, a propuesta de la persona titular de la Presidencia del Comité.

Disposición transitoria única. Mantenimiento de funciones y responsabilidades.

Los agentes que a la fecha de entrada en vigor de esta orden conformen la estructura organizativa de la seguridad de la información en la Consejería mantendrán sus funciones y responsabilidades, de manera transitoria, hasta la efectiva constitución del nuevo Comité de Seguridad de la Información y la designación de nuevos agentes que sean requeridas por esta política de seguridad de la información.

Disposición derogatoria única. Derogación de normas.

Quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo establecido en la presente orden y, en particular, la Orden de 30 de marzo de 2021, por la que se establece la política de seguridad de la información de la Consejería de Agricultura, Ganadería, Pesca y Desarrollo Sostenible, salvo por su posible utilización con carácter transitorio por la Consejería de Sostenibilidad y Medio Ambiente en base a la disposición transitoria quinta del Decreto 162/2022, de 9 de agosto, por el que se establece su estructura orgánica, modificado por el Decreto 170/2024, de 26 de agosto.

Disposición final primera. Habilitación para ejecución y desarrollo.

Se habilita a la persona titular del órgano directivo de la Consejería con competencias en materia de seguridad de la información para dictar cuantas actuaciones sean necesarias para la ejecución y desarrollo de lo establecido en la presente orden.

Disposición final segunda. Entrada en vigor.

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

Sevilla, 5 de noviembre de 2024

RAMÓN FERNÁNDEZ-PACHECO MONTERREAL
Consejero de Agricultura, Pesca, Agua
y Desarrollo Rural

00310779