3. Otras disposiciones

CONSEJERÍA DE FOMENTO, INFRAESTRUCTURAS Y ORDENACIÓN DEL TERRITORIO

Orden de 21 de enero de 2022, por la que se modifica la Orden de 23 de julio de 2019, por la que se aprueba el documento de Política de Seguridad de las Tecnologías de la Información y Comunicaciones y de la protección de datos de carácter personal de la Consejería de Fomento, Infraestructuras y Ordenación del Territorio.

Mediante Orden de esta Consejería, de fecha 23 de julio de 2019, se aprueba documento de Política de Seguridad de las Tecnologías de la Información y Comunicaciones y de la protección de datos de carácter personal de la Consejería de Fomento, Infraestructuras y Ordenación del Territorio, que se insertaba a continuación. Y ello en cumplimiento de lo establecido en el artículo 10 del Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía, modificado por el Decreto 70/2017, de 6 de junio, y de cuyo tenor , en cada entidad incluida en el ámbito de aplicación del Decreto se creará un Comité de Seguridad TIC, como órgano de dirección y seguimiento en materia de seguridad de los activos TIC de su titularidad o cuya gestión tenga encomendada. Asimismo, en el apartado 2 de este mismo artículo se prevé que la composición, atribuciones, funcionamiento y método de trabajo del Comité de Seguridad TIC de las entidades incluidas en el ámbito de aplicación del presente decreto deberá ser aprobada por el máximo órgano de dirección de la entidad, en el caso de las Consejerías mediante Orden de la persona titular de la misma.

Por otro lado, 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, tiene por objeto el establecimiento de una política de Seguridad Interior en la Administración de la Junta de Andalucía que defina un completo sistema para la prevención y reacción ante daños intencionadamente provocados por agentes externos, personal propio o personas usuarias, contra sus propias personas usuarias, su personal, sus activos y la continuidad de su funcionamiento y servicios.

En este decreto, y sobre la base de los principios de simplificación, economía, eficacia y eficiencia administrativa, se ha optado por evitar la creación ex novo de un Comité para la seguridad Interior en cada Consejería o entidad, optando por incluir las que hubiesen sido sus funciones y tareas, en los Comités de Seguridad TIC previamente creados según la normativa antes citada. De esta forma, el artículo 9 del Decreto 171/2020, de 13 de octubre, dispone que, en cada Consejería o entidad dependiente, existirá un Comité de Seguridad Interior y Seguridad TIC, integrando las funciones y responsabilidades que se determinan en los respectivos Decretos para este tipo de órganos de dirección. En concreto, el artículo 9 del mencionado Decreto 171/2020, de 13 de octubre, prevé que Las respectivas normas de creación de los Comités a los que alude el artículo 10 del Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones de la Administración de la Junta de Andalucía, modificarán su denominación añadiendo su definición como órganos de dirección y seguimiento en materia de seguridad interior y actualizando, de ser necesario, la composición y régimen de los mismos, con descripción incluso, de las nuevas funciones a incorporar.

A tal fin, en los casos de que el Comité de Seguridad TIC estuviese ya creado por norma habilitante y publicada en el Boletín Oficial de la Junta de Andalucía, deberá procederse a modificar su denominación, su composición y sus funciones para adecuarse también a las políticas de seguridad interior de la entidad, en el marco de la política de Seguridad Interior de la Administración de la Junta de Andalucía.

00254276

Es más, según consta en acta de fecha del 27 de octubre de 2020, y en virtud de lo dispuesto en la Orden de 23 de julio de 2019, por la que se aprueba el documento de Política de Seguridad de las Tecnologías de la Información y Comunicaciones y de la protección de datos de carácter personal de la Consejería de Fomento, Infraestructuras y Ordenación del Territorio, se constituye el Comité de Seguridad Interior y Seguridad TIC de la Consejería, como órgano de dirección y seguimiento en materia de seguridad de estos activos en el ámbito de la Consejería. En la misma acta se indica expresamente que la entrada en vigor 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, ha ampliado las competencias y modificado la denominación de este Comité, el cual pasa a llamarse Comité de Seguridad Interior y Seguridad TIC, sin perjuicio de las modificaciones normativas futuras que deban producirse para la adaptación a este decreto.

De esta manera y en base de cuanto antecede, la presente modificación puntual de la Orden de 23 de julio de 2019 responde al mandato reglamentario contenido en el Decreto 171/2020, de 13 de octubre y cuyo objetivo es adaptar el actual Comité de Seguridad TIC a su nueva denominación y definición como órgano de dirección y seguimiento en materia de seguridad interior además de actualizar su composición y la descripción de las nuevas funciones que debe integrar.

Por tanto, la presente orden cumple con los principios de buena regulación a los que se refiere el artículo 129 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y el artículo 7 del Decreto 622/2019, de 27 de diciembre, de administración electrónica, simplificación de procedimientos y racionalización organizativa de la Junta de Andalucía. En cumplimiento del principio de necesidad, la presente orden responde al mandato de una norma superior, siendo además coherente con el resto del ordenamiento jurídico e integrada en el mismo. Es eficaz y proporcional ya que evita la duplicidad de órganos y, asimismo, es eficiente y su aplicación no impone cargas administrativas innecesarias o accesorias. Por otro lado, al tratarse de una norma organizativa que no afecta directamente a los derechos e intereses legítimos de la ciudadanía, se ha prescindido de los trámites de consulta, audiencia e información públicas previstos en el artículo 133 de la Ley 39/2019, de 1 de octubre.

En su virtud, a propuesta de la Secretaria General Técnica, conforme a lo establecido en el Decreto 107/2019, de 12 de febrero, por el que se establece la estructura orgánica de la Consejería de Fomento, Infraestructuras y Ordenación del Territorio, modificado por el Decreto 440/2019, de 2 de abril, 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

Artículo único. Modificación de la Orden de 23 de julio de 2019, por la que se aprueba el documento de Política de Seguridad de las Tecnologías de la Información y Comunicaciones y de la protección de datos de carácter personal de la Consejería de Fomento, Infraestructuras y Ordenación del Territorio.

1. La Orden de 23 de julio de 2019, por la que se aprueba el documento de Política de Seguridad de las Tecnologías de la Información y Comunicaciones y de la protección de datos de carácter personal de la Consejería de Fomento, Infraestructuras y Ordenación del Territorio, pasa a denominarse «Orden de 23 de julio de 2019, por la que se aprueba el documento de Política de Seguridad y de la protección de datos de carácter personal de la Consejería de Fomento, Infraestructuras y Ordenación del Territorio» y queda modificada como sigue:

00254276

Uno. El artículo 1 queda redactado del siguiente modo:

«Artículo 1. Aprobación del Documento de Política de Seguridad y de la protección de datos de carácter personal de la Consejería de Fomento, Infraestructuras y Ordenación del Territorio.

Se aprueba el Documento de Política de Seguridad y de la protección de datos de carácter personal de la Consejería de Fomento, Infraestructuras y Ordenación del Territorio, que se inserta a continuación.»

Dos. El artículo 2 queda redactado del siguiente modo:

«Artículo 2. Creación del Comité de Seguridad Interior y Seguridad TIC de la Consejería de Fomento, Infraestructuras y Ordenación del Territorio.

Se crea el Comité de Seguridad Interior y Seguridad TIC de la Consejería de Fomento, Infraestructuras y Ordenación del Territorio, como órgano de dirección y seguimiento en materia de seguridad interior y protección de datos personales, de los activos TIC que sean de su titularidad o cuya gestión tenga encomendada. Su alcance está delimitado exclusivamente al ámbito de la Consejería.»

2. El Documento de Política de Seguridad de las Tecnologías de la Información y Comunicaciones (TIC) y de la protección de datos de carácter personal de la Consejería de Fomento, Infraestructuras y Ordenación del Territorio, pasa a denominarse «Documento de Política de Seguridad y de la protección de datos de carácter personal de la Consejería de Fomento, Infraestructuras y Ordenación del Territorio» y queda modificado como sigue:

Uno. El apartado 1 queda redactado del siguiente modo:

«1. Objeto y definiciones.

El presente documento tiene por objeto definir la política de seguridad interior, de seguridad de las Tecnologías de la Información y Comunicaciones (en adelante, TIC) y de la protección de datos de carácter personal de la Consejería de Fomento, Infraestructuras y Ordenación del Territorio, incluyendo el marco organizativo y tecnológico aplicable, conforme a la política en materia de seguridad interior y de seguridad de las Tecnologías de la Información y Comunicaciones de la Administración de la Junta de Andalucía, a su marco específico regulador de la seguridad interior y de seguridad TIC y de la protección de datos de carácter personal, y a la normativa general vigente en estas materias.

A los efectos de lo previsto 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, en materia de política de seguridad interior, se asumen las definiciones establecidas en el artículo 3 del citado decreto.»

Dos. El apartado 2 queda redactado del siguiente modo:

«2. Alcance y ámbito de aplicación.

El Decreto 1/2011, de 11 de enero, de la Consejería de Empleo Empresa y Comercio, 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, modificado por el Decreto 70/2017, de 6 de junio, de la Consejería de Empleo, Empresa y Comercio, en su Anexo I define la política de seguridad de la información y comunicaciones como el “conjunto de directrices plasmadas en un documento escrito, que rigen la forma en que una organización gestiona y protege sus activos de tecnologías de la información y comunicaciones”, y considera estos activos TIC, como “cualquier información o sistema de información que tenga valor para la organización”, incluyendo “datos, servicios, aplicaciones, equipos, comunicaciones, instalaciones, procesos y recursos humanos”.

La presente política de la Consejería se aplicará a los activos TIC de su titularidad o cuya gestión tenga encomendada, y su ámbito de aplicación se extenderá a la protección

00254276

de datos de carácter personal, en lo que a la Consejería le afecte en cumplimiento de la normativa vigente en esta materia.

La información en soporte papel, de valor para la organización, o el tratamiento no automatizado de datos personales, se consideran por tanto, dentro del ámbito de aplicación de esta política.

A fin de garantizar un enfoque de seguridad integral, se establecerán mecanismos de coordinación con aquellas áreas que, sin guardar una relación directa con la seguridad TIC y protección de datos personales, incidan de algún modo en ellas.

La política de seguridad TIC y de la protección de datos de carácter personal será de aplicación a la Consejería de Fomento, Infraestructuras y Ordenación del Territorio, tanto a sus Servicios Centrales como periféricos.

De conformidad con el artículo 10.3 del citado Decreto 1/2011, de 11 de enero, la presente política de seguridad y sus documentos complementarios también serán de obligado cumplimiento para sus entidades vinculadas o dependientes.

En materia de política de seguridad interior, esta orden será de aplicación a los servicios centrales, y periféricos de la Consejería de Fomento, Infraestructuras y Ordenación del Territorio, de acuerdo con lo dispuesto en el Decreto 107/2019, de 12 de febrero, modificado por el Decreto 440/2019, de 2 de abril, por el que se establece la estructura orgánica de la Consejería de Fomento, Infraestructuras y Ordenación del Territorio.

Cada una de las entidades instrumentales de la Consejería deberá disponer formalmente de su propio documento de política interior y de seguridad TIC, de acuerdo con lo establecido en el artículo 10.1 del Decreto 1/2011, de 11 de enero y en los artículos 1 y 2 del Decreto 171/2020, de 13 de octubre.»

Tres. El apartado 3 queda redactado del siguiente modo:

«3. Objetivos.

La política de seguridad de las tecnologías de la información y comunicaciones y de la protección de datos de la Consejería de Fomento, Infraestructuras y Ordenación del Territorio tiene como objetivos los siguientes:

a) Garantizar la seguridad de los activos TIC y en particular, la protección de datos de carácter personal en su ámbito de aplicación.

b) Garantizar a toda la ciudadanía andaluza que, en el ámbito de la Consejería, sus datos y, en particular, los tratamientos de aquellos de carácter personal, serán gestionados y protegidos de acuerdo a los estándares y buenas prácticas en seguridad TIC y en protección de datos personales, así como a lo exigido en la legislación vigente en estas materias.

c) Aumentar el nivel de concienciación en la Consejería en materia de seguridad TIC y protección de datos de carácter personal, garantizando que el personal a su servicio es consciente de sus obligaciones y responsabilidades.

d) Establecer la estructura de la organización de la seguridad TIC y de protección de datos de carácter personal de la Consejería.

e) Establecer las directrices, los objetivos y los principios básicos de seguridad TIC de la Consejería.

f) Establecer las bases de desarrollo de la política de la seguridad TIC y de la protección de datos de carácter personal de la Consejería, para la elaboración de normas, procedimientos y documentación técnica relacionada.

g) Establecer un modelo integral de gestión de la seguridad TIC y de la protección de datos de carácter personal en la Consejería, basado en la gestión de riesgos del Esquema Nacional de Seguridad, que cubra en un ciclo continuo de mejora los aspectos técnicos, organizativos y procedimentales.

h) Garantizar el cumplimiento de la legislación vigente en materia de seguridad TIC y protección de datos de carácter personal.

00254276

En materia de política de seguridad interior y a los efectos de lo previsto 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, se asumen los objetivos establecidos en el artículo 4 del citado decreto.»

Cuatro. El apartado 4 queda redactado del siguiente modo:

«4. Principios.

Los principios básicos que rigen la política de la seguridad TIC y de la protección de datos de carácter personal de la Consejería, se encuentran inspirados y alineados con los recogidos en la normativa reguladora de la política de seguridad TIC de la Administración de la Junta de Andalucía, del Esquema Nacional de Seguridad y de la protección de datos de carácter personal. De acuerdo con ello, con carácter general, la política de la seguridad TIC y de la protección de datos de carácter personal de la Consejería se desarrollará de acuerdo a los siguientes principios básicos:

a) Principio de gestión integral de seguridad TIC y protección de datos de carácter personal.

La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema, excluyendo cualquier actuación puntual o tratamiento coyuntural.

b) Principio de confidencialidad.

Los activos TIC deberán ser accesibles únicamente para aquellas personas usuarias, órganos y entidades o procesos expresamente autorizados para ello, con respeto a las obligaciones de secreto y sigilo profesional.

c) Principio de integridad y calidad.

Se deberá garantizar el mantenimiento de la integridad y calidad de la información, así como de los procesos de tratamiento de la misma, estableciéndose los mecanismos para asegurar que los procesos de creación, tratamiento, almacenamiento y distribución de la información contribuyen a preservar su exactitud y corrección.

d) Principio de gestión del riesgo.

Se deberá articular un proceso continuo y permanentemente actualizado, de análisis y tratamiento de riesgos como mecanismo básico sobre el que debe descansar la gestión de la seguridad de los activos TIC. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad.

e) Principio de proporcionalidad en coste.

La implantación de medidas que mitiguen los riesgos de seguridad de los activos TIC deberá hacerse bajo un enfoque de proporcionalidad en los costes económicos y operativos.

f) Principio de concienciación y formación.

Se articularán iniciativas que permitan a las personas usuarias conocer sus deberes y obligaciones en cuanto al tratamiento seguro de la información se refiere. De igual forma, se fomentará la formación específica de todas aquellas personas que gestionan y administran sistemas de información y telecomunicaciones, o realizan actividades que guarden relación con el tratamiento de datos de carácter personal, en las materias de seguridad TIC y protección de datos de carácter personal que correspondan.

g) Principio de prevención.

Se desarrollarán planes y líneas de trabajo específicas orientadas a evitar, o al menos prevenir en la medida de lo posible, fraudes, incumplimientos o incidentes relacionados con la seguridad TIC y la protección de datos de carácter personal. 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

00254276

evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, estarán claramente definidos y documentados.

h) Principio de detección.

Se desarrollarán líneas de trabajo específicas orientadas a la detección de fraudes, incumplimientos o incidentes relacionados con la seguridad TIC y la protección de datos de carácter personal. La operación de los servicios debe monitorizarse de manera continua para detectar anomalías en los niveles de prestación requeridos, desde una simple degradación a la detención de los mismos, actuando en consecuencia.

La monitorización es especialmente relevante para permitir el establecimiento de 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 que se hayan preestablecido como normales.

i) Principio de reacción.

Se establecerán mecanismos para responder eficazmente a los incidentes de seguridad, designando un punto de contacto para las comunicaciones con respecto a incidentes de seguridad TIC y de protección de datos de carácter personal, así como estableciendo protocolos para el intercambio de información relacionada con dichos incidentes.

j) Principio de recuperación, disponibilidad y continuidad.

Deberá minimizarse el tiempo requerido de recuperación, de forma que el impacto de los incidentes de seguridad sea el menor posible. Se garantizará un alto nivel de disponibilidad en los activos TIC y se dotarán de los planes y medidas necesarias para asegurar la continuidad de los servicios y la recuperación ante posibles contingencias graves.

k) Principio de mejora continua.

Se revisará el grado de eficacia de los controles de seguridad TIC implantados, al objeto de adecuarlos a la constante evolución de los riesgos y del entorno tecnológico de la Consejería.

l) Principio de seguridad TIC y de protección de datos de carácter personal durante todo el ciclo de vida de los activos TIC.

Las especificaciones de seguridad se incluirán en todas las fases del ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.

En cuanto a la protección de datos personales, ésta se garantizará desde el diseño y por defecto. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, 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, 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 y que los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

m) Principio de responsabilidad.

Las obligaciones y responsabilidades que correspondan en seguridad TIC y protección de datos de carácter personal se determinarán y serán comunicadas de forma explícita a las personas implicadas.

La responsabilidad de la seguridad TIC estará diferenciada de la responsabilidad sobre la prestación de los servicios.

n) Principios de licitud, lealtad y transparencia, relativos al tratamiento de datos personales.

Los datos personales serán tratados de manera lícita, leal y transparente en relación con el interesado.

00254276

o) Principio de limitación de la finalidad, en relación al tratamiento de datos personales.

Los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines.

p) Principio de minimización de datos, en relación al tratamiento de datos personales.

Los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.

q) Principio de exactitud, relativo al tratamiento de datos personales.

Los datos personales serán exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan.

r) Principio de limitación del plazo de conservación, en relación al tratamiento de datos personales.

Los datos personales serán mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales.

s) Principio de integridad y confidencialidad, en relación al tratamiento de datos personales.

Los datos personales serán tratados de tal manera que se garantice una seguridad adecuada de los datos personales, 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.

t) Principio de responsabilidad proactiva, relativo al tratamiento de datos personales.

El responsable del tratamiento será responsable del cumplimiento de los principios relativos al tratamiento de datos personales y capaz de demostrarlo.

En materia de política de seguridad interior y a los efectos de lo previsto 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, se asumen los principios establecidos en el artículo 5 del citado decreto.»

Cinco. El apartado 5 queda redactado del siguiente modo:

«5. Marco regulador de referencia.

La política de seguridad interior, de seguridad TIC y de protección de datos de carácter personal de la Consejería de Fomento, Infraestructuras y Ordenación del Territorio y su normativa de desarrollo, se establecen de conformidad con la política de seguridad interior y de seguridad de las Tecnologías de la Información y Comunicaciones de la Administración de la Junta de Andalucía y su marco regulador específico en el ámbito de la seguridad TIC y la protección de datos de carácter personal, así como con la normativa general y vigente relacionada con ambas materias.

Entre la normativa genérica de referencia para la política de seguridad interior, de seguridad TIC y de la protección de datos de carácter personal de la Consejería y su normativa de desarrollo, sobresalen:

- El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, modificado por el Real Decreto 951/2015, de 23 de octubre .

- 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 .

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

El marco regulador específico de seguridad interior y de seguridad TIC y de protección de datos de carácter personal de la Administración de la Junta de Andalucía, está constituido por las siguientes disposiciones y documentos:

00254276

- 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 sus Órdenes de desarrollo, modificado por el 70/2017, de 6 de junio.

- 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 y sus posteriores normas de desarrollo.

- Resoluciones de la Dirección General 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.

- Disposiciones del órgano competente en materia de protección de datos en el ámbito de la Administración de la Junta de Andalucía.

- Documentos técnicos, que se agrupan en las categorías de procedimientos y guías técnicas.»

Seis. El apartado 6 pasa a denominarse “Organización de la seguridad interior y de la seguridad TIC y de la protección de datos de carácter personal de la Consejería”, cuyos números 6.1, 6.2.1, 6.2.2, 6.2.3, 6.2.4 , 6.7 y 6.12 quedan redactados del siguiente modo:

«6.1. Estructura organizativa.

La organización de la Seguridad Interior y Seguridad TIC y de la protección de datos de carácter personal de la Consejería está compuesta por la siguiente estructura:

- Comité de Seguridad Interior y Seguridad TIC de la Consejería.
- Responsables de la Información.
- Responsables de los Servicios.
- Responsables de Sistemas.
- Unidad de Seguridad TIC.
- Unidad de Seguridad Interior.
- Puntos Coordinadores de Seguridad Interior.
- Responsables de los tratamientos de datos de carácter personal.
- Encargados de los tratamientos de datos de carácter personal.
- Delegado de Protección de Datos.

Bajo esta estructura organizativa, adicionalmente, cabe conformar cuantos grupos técnicos se consideren apropiados, a fin de lograr un mejor desempeño de las funciones para la gestión de la seguridad interior, la seguridad TIC y la protección de datos personales.

De conformidad con el artículo 10.1 del Decreto 1/2011, de 11 de enero y el artículo 9 del Decreto 171/2020, de 13 de octubre, cada una de las entidades instrumentales de la Consejería, deberá contar con un Comité de Seguridad Interior y de Seguridad TIC que actuará como órgano de dirección y seguimiento en materia de seguridad interior, de seguridad de los activos TIC y protección de datos personales de su titularidad o cuya gestión tenga encomendada.»

«6.2.1. Objeto y alcance.

El Comité de Seguridad Interior y Seguridad TIC de la Consejería actuará como órgano de dirección y seguimiento en materia de seguridad interior, seguridad y protección de datos personales, de los activos de seguridad interior y activos TIC de su titularidad o cuya gestión tenga encomendada. Su alcance estará delimitado exclusivamente al ámbito de la Consejería.

En los apartados siguientes, se describe su composición, atribuciones y régimen de funcionamiento.»

«6.2.2. Composición.

El Comité de Seguridad Interior y Seguridad TIC de la Consejería estará compuesto por los siguientes miembros:

a) Presidencia (con voz y voto): La persona titular de la Viceconsejería.

b) Vicepresidencia (con voz y voto): La persona titular de la Secretaría General Técnica.

00254276

c) Vocalías de órganos directivos de la Consejería (con voz y voto): Las personas titulares de todos los órganos directivos centrales y periféricos y la persona titular de la Coordinación General de la Secretaría General Técnica.

d) Vocalías asesoras (con voz, pero sin voto): La persona titular de la Unidad Administrativa responsable de Informática, la persona titular de la Unidad de Seguridad TIC, la persona titular de la Unidad de Seguridad Interior y la persona que ostente la condición de Delegado de Protección de Datos.

e) Secretaría (sin voz y sin voto): Será ejercida por una persona de la Consejería designada por la Presidencia del Comité.

El régimen de suplencias, en caso de vacante, ausencia o enfermedad u otras causas legales será el siguiente:

- La persona titular de la Presidencia será sustituida por la persona titular de la Vicepresidencia.
- Tanto la Vicepresidencia como cada una de las Vocalías de órganos directivos de la Consejería, podrán designar una persona que les sustituya en estas circunstancias, entre personal funcionario que ocupe puestos de trabajo de nivel 28 o superior.

La composición del Comité de Seguridad Interior y de Seguridad TIC deberá respetar la representación equilibrada de mujeres y hombres.

El Comité de Seguridad Interior y Seguridad TIC podrá convocar a sus reuniones, con voz y sin voto a las personas que en cada caso autorice la presidencia por propia iniciativa o a propuesta de alguno de sus miembros. En particular, podrá utilizarse este mecanismo a fin de facilitar la colaboración y la coordinación con las entidades vinculadas o dependientes de la Consejería. Asimismo podrá recabar de personal técnico especializado, propio o externo, la información pertinente para la toma de decisiones.»

«6.2.3. Atribuciones.

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

Son funciones propias del Comité de Seguridad Interior y Seguridad TIC, en materia de Seguridad Interior:

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

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

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

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

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

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

g) La designación de la Unidad de Seguridad Interior.

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

Son funciones propias del Comité de Seguridad Interior y Seguridad TIC, en materia de Seguridad TIC:

a) Velar por el cumplimiento de la política de la seguridad TIC y de la protección de datos de carácter personal de la Consejería, así como de su desarrollo normativo.

00254276

b) Impulsar la implantación, concienciación, formación, divulgación, actualización y el desarrollo normativo de la política de la seguridad TIC y de la protección de datos de carácter personal.

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

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

e) Aprobar el desarrollo de segundo nivel de la política de seguridad TIC y de la protección de datos de carácter personal, según lo previsto en el apartado 8.2.

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

g) Velar para que todos los ámbitos de responsabilidad y actuación en relación a la seguridad TIC y la protección de datos de carácter personal queden perfectamente definidos, asegurando que todos y cada uno de los miembros de la estructura de seguridad definida conozcan sus funciones y responsabilidades y aprobando los nombramientos necesarios para ello. En particular, el Comité nombrará la Unidad de Seguridad TIC de la Consejería cuya persona responsable ostentará la condición de Responsable de Seguridad TIC de la Consejería.

h) Resolver los conflictos que puedan aparecer entre las diferentes personas responsables o entre diferentes áreas de la organización en materia de seguridad TIC y protección de datos personales, en los casos señalados en el apartado 6.11.

i) Velar porque la seguridad TIC se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación y, en el caso de datos de carácter personal, como se establece en el Reglamento General de Protección de Datos, que estos sean protegidos desde el diseño y por defecto. También deberá velar por que el desarrollo normativo que tenga incidencia en el desarrollo o explotación de sistemas de información se adecúa a lo establecido en la presente política de seguridad, promoviendo la creación y utilización de servicios horizontales que, desde la perspectiva de la seguridad TIC y la protección de datos personales, reduzcan duplicidades y contribuyan a un funcionamiento homogéneo de todos los sistemas TIC.

j) Promover y fomentar la divulgación y formación en cultura de la seguridad TIC y protección 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.

k) Coordinar las medidas técnicas y organizativas establecidas en 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 del Delegado de Protección de Datos.

l) Realizar el seguimiento de los principales riesgos residuales asumidos por la organización en el ámbito de la seguridad TIC y la protección de datos personales, y aprobar posibles actuaciones respecto de ellos.

m) Promover y coordinar a alto nivel la realización de auditorías que correspondan, en el ámbito de la seguridad TIC y la protección de datos de carácter personal, y aprobar las actuaciones correspondientes que se propongan, a partir de sus conclusiones y recomendaciones.

n) Velar por la coordinación a alto nivel en la gestión de incidentes de seguridad TIC y de protección de datos personales y aprobar las actuaciones que sean pertinentes.

00254276

ñ) Establecer los mecanismos necesarios para compartir la documentación derivada del desarrollo normativo, así como sus medios de difusión.

o) Aprobar el Registro de actividades de tratamiento de la Consejería así como sus modificaciones.

La Presidencia del Comité de Seguridad Interior y Seguridad TIC ostenta la representación del Comité de Seguridad Interior y Seguridad TIC correspondiéndole:

- Acordar la convocatoria de las reuniones ordinarias y extraordinarias y establecer el orden del día de las mismas, a partir de las peticiones de los demás miembros.
- Presidir las reuniones, moderar los debates y suspenderlos por causas justificadas.
- Dirimir con su voto de calidad los empates en votaciones para la adopción de acuerdos.
- Certificar los acuerdos del Comité.

La Secretaría realiza las convocatorias de las reuniones por orden de la Presidencia del Comité, así como las citaciones al resto de miembros del Comité. También se encarga de elaborar las actas de las reuniones y los acuerdos adoptados.»

«6.2.4. Funcionamiento del Comité de Seguridad Interior y Seguridad TIC de la Consejería.

El Comité de Seguridad Interior y Seguridad TIC de la Consejería se regirá por lo indicado en el presente documento de política de seguridad, así como por la normativa reguladora de la política de seguridad interior y seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía, y por el resto de normativa aplicable, como la reguladora del Esquema Nacional de Seguridad y la normativa de protección de datos de carácter personal.

El Comité de Seguridad Interior y Seguridad TIC de la Consejería se reunirá con carácter ordinario dos veces al año y con carácter extraordinario por acuerdo de la presidencia.

El Comité se podrá constituir, convocar, celebrar sus sesiones, adoptar acuerdos y remitir actas, tanto de forma presencial como utilizando redes de comunicación a distancia, con las medidas adecuadas que garanticen la identidad de las personas comunicantes y la autenticidad de la información entre ellas transmitida.

El quorum necesario para la celebración de una reunión del Comité es la mitad más uno de los miembros que componen el Comité, siendo obligatoria la presencia de la persona titular de la Presidencia y de la Secretaría o suplentes en su caso, y una de entre las personas que ostente la condición de Delegado de Protección de Datos o de responsable de la Unidad de Seguridad TIC o responsable de la Unidad de Seguridad Interior, en atención a la naturaleza de los temas que se vayan a tratar.

Los miembros del Comité de Seguridad Interior y Seguridad TIC podrán individual o colectivamente, proponer a la Presidencia de forma motivada, la inclusión de determinados asuntos en el orden del día de una reunión ordinaria. La propuesta deberá realizarse mediante medio electrónico, dirigido a la Presidencia con una antelación mínima de 3 días laborables a la fecha de la convocatoria.

Los miembros del Comité de Seguridad Interior y Seguridad TIC también podrán individual o colectivamente, proponer a la Presidencia de forma motivada, la celebración de una reunión extraordinaria, así como los asuntos a tratar en la misma. La propuesta deberá realizarse mediante medio electrónico, dirigido a la Presidencia, con una antelación mínima de 10 días laborables siempre que la reunión no tenga un carácter urgente, en cuyo caso se requerirá una antelación mínima de 8 horas.

Las propuestas de acuerdos del Comité de Seguridad Interior y Seguridad TIC serán sometidas a votación y estos se adoptarán por mayoría simple de los miembros presentes en la reunión.

En caso de empate, se realizará una nueva votación, y si este persistiera, decidirá el voto de calidad de la Presidencia.

00254276

Una vez aprobada y publicada la presente política de seguridad, la primera reunión del Comité de Seguridad Interior y Seguridad TIC de la Consejería tendrá por objeto su constitución y se procederá al nombramiento de la Unidad de Seguridad TIC y de la Unidad de Seguridad Interior, mediante la respectiva designación de sus personas responsables, así como al nombramiento de los Responsables de la Información y de los Servicios.»

«6.7. La Unidad de Seguridad Interior y la Unidad de Seguridad TIC .

6.7.1. Unidad de Seguridad Interior.

En virtud del artículo 10.1 del Decreto 171/2020, de 13 de octubre, la Consejería contará con una Unidad de Seguridad Interior que ejercerá la responsabilidad ejecutiva para la seguridad interior del conjunto de los activos de su ámbito.

La persona responsable de la unidad, tendrá la condición de responsable de seguridad interior, y su designación se realizará por el Comité de Seguridad Interior y Seguridad TIC entre el personal funcionario al servicio de la Consejería.

La Unidad de Seguridad Interior de la Consejería tendrá las siguientes atribuciones, de acuerdo con lo dispuesto en el artículo 10.2 del Decreto 171/2020, de 13 de octubre:

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

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

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

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

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

f) La coordinación y el seguimiento de la actividad de los puntos coordinadores responsables de seguridad interior de la Consejería.

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

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

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

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

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

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

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

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

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

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

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

00254276

6.7.2. Unidad de Seguridad TIC.

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

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

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

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

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

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

e) Definición y supervisión de los criterios y requisitos técnicos de seguridad aplicados en las distintas fases del ciclo de vida de los soportes, sistemas y aplicaciones de la Consejería por parte de los Servicios o Departamentos responsables de la prestación de los servicios de tecnologías de la información y comunicaciones. Antes de la puesta en producción de nuevos sistemas de información o de evolutivos de los existentes, la Unidad de Seguridad TIC deberá evaluar los aspectos de seguridad y comunicar los posibles riesgos a los Responsables de la Información y Responsables de los Servicios correspondientes.

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

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

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

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

«6.12. Cooperación con otros órganos y otras Administraciones en materia de seguridad interior y seguridad TIC y protección de datos personales.

A efectos de coordinación, obtención de asesoramiento e intercambio de experiencias para la mejora continua de la gestión de la seguridad, se fomentará el establecimiento de mecanismos de comunicación con otros agentes especializados en esta materia. En especial, se contemplarán los siguientes:

- Comité Corporativo de Seguridad Interior de la Junta de Andalucía.
- Comité de Seguridad TIC de la Junta de Andalucía.
- Unidad Corporativa de Seguridad Interior.
- Unidad de Seguridad TIC Corporativa de la Junta de Andalucía.
- Consejo de Transparencia y Protección de Datos de Andalucía.
- CCN-CERT: Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional (CCN), como soporte y coordinación para la resolución de incidentes que sufra la Administración General, Autonómica o Local.

00254276

- Agencia Española de Protección de Datos (AEPD).
- Instituto Nacional de Ciberseguridad (INCIBE).
- Grupo de Delitos Informáticos y Telemáticos de la Guardia Civil y Brigada de Investigación Tecnológica (BIT) del Cuerpo Nacional de Policía, para la investigación de acciones relacionadas con la delincuencia informática y los fraudes en el sector de las telecomunicaciones.»

Siete. El apartado 9 queda redactado del siguiente modo:

«9. Obligaciones sobre el conocimiento y cumplimiento de la política de seguridad

9.1. Obligaciones del personal y terceras partes.

Los objetivos de la política de seguridad interior, de la seguridad TIC y la protección de datos de carácter personal de la Consejería, serán considerados objetivos comunes a 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 seguridad interior y activos TIC puestos a su disposición.

Tanto el personal de la Consejería de Fomento, Infraestructuras y Ordenación del Territorio, como aquel que preste servicios en la misma, tiene la obligación de conocer y cumplir la presente política de seguridad y su normativa de desarrollo, siendo responsabilidad del Comité de Seguridad Interior y Seguridad TIC disponer los medios necesarios para que la información llegue a dichas personas.

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

Cuando la Consejería de Fomento, Infraestructuras y Ordenación del Territorio preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta política de seguridad, 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.

Cuando la Consejería de Fomento, Infraestructuras y Ordenación del Territorio utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta política de seguridad y de la normativa de seguridad interior, de seguridad TIC y de protección de datos personales que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta, a través de cláusulas contractuales o acuerdos de nivel servicio, a las obligaciones generales establecidas en dicha normativa, pudiendo disponer la tercera parte de sus propios procedimientos operativos para satisfacerla. 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 la presente política de seguridad.

Cuando algún aspecto de esta política de seguridad no pueda ser satisfecho por una tercera parte según se requiere en el párrafo anterior, se requerirá un informe de la Unidad de Seguridad Interior o de la Unidad de Seguridad TIC, en función de la materia y con asesoramiento del Delegado de Protección de Datos en el caso de que se vean afectados datos de carácter personal, que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y/o los servicios afectados antes de proseguir en la relación con la tercera parte.

9.2. Exigencia de responsabilidades.

La Consejería de Fomento, Infraestructuras y Ordenación del Territorio procederá el ejercicio de las acciones pertinentes para la exigencia de las responsabilidades legales que correspondan por el incumplimiento manifiesto de seguridad interior , de la política de seguridad TIC o de la normativa de seguridad derivada.

00254276

9.3. Formación y concienciación.

La Consejería desarrollará actividades de formación y concienciación en materias de seguridad interior, de seguridad TIC y protección de datos de carácter personal, destinadas a las personas empleadas públicas de los órganos contemplados en el ámbito de aplicación de esta norma.»

Disposición adicional única. Adaptación de la denominación del Comité de Seguridad de las Tecnologías de la Información y Comunicaciones (Comité de Seguridad TIC), de la Consejería de Fomento, Infraestructuras y Ordenación del Territorio.

En la Orden de 23 de julio de 2019, por la que se aprueba el documento de Política de Seguridad de las Tecnologías de la Información y Comunicaciones y de la protección de datos de carácter personal de la Consejería de Fomento, Infraestructuras y Ordenación del Territorio y en el propio documento insertado a continuación, todas las alusiones en el texto al «Comité de Seguridad de las Tecnologías de la Información y Comunicaciones (Comité de Seguridad TIC), de la Consejería de Fomento, Infraestructuras y Ordenación del Territorio» quedan sustituidas por «Comité de Seguridad Interior y Seguridad TIC de la Consejería de Fomento, Infraestructuras y Ordenación del Territorio».

Disposición final única. Entrada en vigor.

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

Sevilla, 21 de enero de 2022

MARÍA FRANCISCA CARAZO VILLALONGA
Consejera de Fomento, Infraestructuras
y Ordenación del Territorio

00254276