3. Otras disposiciones

CONSEJERÍA DE FOMENTO, INFRAESTRUCTURAS Y ORDENACIÓN DEL TERRITORIO

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.

Los avances tecnológicos en los ámbitos de la informática, las telecomunicaciones y de la sociedad de la información son ya un hecho consolidado, que afecta no sólo a la sociedad sino también a los poderes públicos. 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. Para conseguir esta confianza, los medios tecnológicos utilizados deben ser seguros y para ello se debe garantizar la confidencialidad, integridad y disponibilidad de los sistemas, de las comunicaciones y de los servicios telemáticos, permitiendo tanto a la ciudadanía, los profesionales y las empresas, como a las Administraciones Públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental. El artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea y el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea establecen que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

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 los ciudadanos y de relación de aquellas entre sí. En concreto, la Ley 39/2015 tiene como uno de sus objetivos centrales regular las relaciones entre las Administraciones y los ciudadanos y empresas, teniendo en cuenta el desarrollo de las tecnologías de la información y comunicación de los últimos años y cómo este desarrollo 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 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.

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 mediante Real Decreto 951/2015, de 23 de octubre, tiene precisamente por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la Ley 40/2015, de 1 de octubre, y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada.

En lo referente a la protección de datos de carácter personal, resultan de aplicación, tanto 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 (en adelante, Reglamento General de Protección de Datos), como la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

00159863

En cuanto al ámbito autonómico, 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.

La política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía quedó establecida mediante el Decreto 1/2011, de 11 de enero, de la Consejería de Economía, Innovación y Ciencia, modificado por el Decreto 70/2017, de 6 de junio, de la Consejería de Empleo, Empresa y Comercio, mientras que a través de la Orden de 9 de junio de 2016, de esta misma Consejería, se efectuó el desarrollo de dicha política.

La modificación del Decreto 1/2011 introdujo cambios en la organización corporativa de la seguridad de las Tecnologías de la Información y Comunicaciones (en adelante, TIC), potenciando la estructura de gobierno mediante la definición de atribuciones específicas a las Consejerías en relación con su propia seguridad y con la de las entidades vinculadas o dependientes de ellas, clarificando la aplicación del principio de función diferenciada y delimitando las funciones que deben desempeñar las distintas áreas implicadas en el mantenimiento de la seguridad, en línea con los perfiles con responsabilidad en seguridad definidos en el Real Decreto 3/2010.

Entre estas atribuciones a las Consejerías se encuentran la de disponer formalmente de su propio documento de política de seguridad de las TIC y de las disposiciones de desarrollo que adecuen, en su caso, las directrices comunes de la Administración de la Junta de Andalucía a sus particularidades, así como la de contar con un Comité de Seguridad TIC.

En base a todo ello, la presente Orden establece la política de seguridad TIC y de protección de datos personales de la Consejería de Fomento, Infraestructuras y Ordenación del Territorio y, por tanto, su compromiso con la seguridad de la información, definiendo objetivos y criterios básicos para su tratamiento, asentando los pilares del marco normativo de seguridad en este organismo y la estructura organizativa y de gestión que velará por su cumplimiento.

La Orden está constituida por dos artículos, en los que se aprueba dicha política y se crea nuevamente el Comité de Seguridad TIC de la Consejería, un documento adjunto que la detalla y una única disposición derogatoria, por la que se derogan todas aquellas disposiciones que contradicen la Orden actual, en particular, las asociadas a la política de seguridad TIC y Comité de seguridad TIC anteriores.

Los apartados 1 a 4 del documento describen el objeto, alcance y principios que rigen la política de seguridad. En los apartados 5 y 6 se define el marco regulador de referencia

00159863

y la estructura organizativa, en la que destaca la incorporación de nuevas figuras responsables como la Unidad de Seguridad TIC, los Responsables de Tratamientos, los Encargados de Tratamientos y el Delegado de Protección de Datos.

El apartado 7 describe el enfoque técnico de referencia de la política de seguridad, encabezado por el Esquema Nacional de Seguridad, y diversos aspectos técnicos destacados de la gestión de la seguridad TIC y la protección de datos personales, como el inventario, clasificación y control de activos TIC, el registro de actividades de tratamientos de datos de carácter personal, la gestión de riesgos, la gestión de incidentes, o las auditorías de seguridad TIC y de la protección de datos personales.

Los apartados 8 a 10 describen las bases para el desarrollo de la política de seguridad TIC y de protección de datos personales de la Consejería y su estructuración en niveles, las obligaciones del personal al respecto, y su política de actualización y difusión.

En la elaboración de esta política de seguridad, se ha tenido en cuenta, además de toda la normativa señalada, el contexto de la Red Corporativa de Telecomunicaciones de la Administración de la Junta de Andalucía, creada por el Acuerdo del Consejo de Gobierno de 2 de junio de 1998, y de los principales sistemas de información corporativos de las entidades que forman parte de la Administración de la Junta de Andalucía.

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

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.

Por ello, 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,

A C U E R D O

Artículo 1. Aprobación del 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 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, que se inserta a continuación.

Artículo 2. Creación 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.

00159863

Se crea el 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, como órgano no colegiado de dirección y seguimiento en materia de seguridad 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.

Disposición derogatoria única.

Quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo establecido en la presente Orden y, en particular, la Resolución de 11 de enero de 2012 de Viceconsejería, por la que se aprueba el Tomo I v3.0 Política de Seguridad, del Documento de Seguridad de los Sistemas de Información de la Consejería de Obras Públicas y Vivienda, y la Orden de 16 de julio de 2013, de la Consejería de Fomento y Vivienda, por la que se crea el Comité de Seguridad de las Tecnologías de la Información y Comunicaciones de la Consejería de Fomento y Vivienda y sus entidades instrumentales.

Disposición final primera. Desarrollo y ejecución.

Se faculta a la persona titular de Viceconsejería y a la persona titular de Secretaría General Técnica de la Consejería de Fomento, Infraestructuras y Ordenación del Territorio para, en el ámbito de sus respectivas competencias, dictar cuantas instrucciones sean necesarias y adoptar cuantas medidas técnicas sean oportunas, para el desarrollo, difusión y ejecución de la presente orden.

Disposición final segunda. Entrada en vigor.

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

Sevilla, 23 de julio de 2019

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

00159863

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

ÍNDICE

00159863

1. Objeto.

El presente documento tiene por objeto definir la política 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 de las Tecnologías de la Información y Comunicaciones de la Administración de la Junta de Andalucía, a su marco específico regulador de la seguridad TIC y de la protección de datos de carácter personal, y a la normativa general vigente en estas materias.

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 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.

Cada una de las entidades instrumentales de la Consejería deberá disponer formalmente de su propio documento de política de seguridad TIC, de acuerdo con el artículo 10.1 de dicho decreto.

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.

00159863

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.

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

00159863

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 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

00159863

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.

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.

5. Marco regulador de referencia.

La política 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 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 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.

00159863

• 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 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:

• 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.

• 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.

6. Organización de la seguridad TIC y de la protección de datos de carácter personal de la Consejería.

6.1. Estructura organizativa.

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

• Comité de Seguridad TIC de la Consejería.
• Responsables de la Información.
• Responsables de los Servicios.
• Responsables de Sistemas.
• Unidad de Seguridad TIC.
• 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 TIC y la protección de datos personales.

De conformidad con el artículo 10.1 del Decreto 1/2011, de 11 de enero, cada una de las entidades instrumentales de la Consejería, deberá contar con un Comité de Seguridad TIC que no tendrá carácter colegiado y que actuará como órgano de dirección y seguimiento en materia de seguridad de los activos TIC y protección de datos personales de su titularidad o cuya gestión tenga encomendada.

6.2. Comité de Seguridad TIC de la Consejería.

6.2.1. Objeto y alcance.

El Comité de Seguridad TIC de la Consejería actuará como órgano no colegiado de dirección y seguimiento en materia de seguridad y protección de datos personales, de los 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 TIC de la Consejería estará compuesto por los siguientes miembros:

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

00159863

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

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 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 por 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.

En la composición del Comité ha de garantizarse, en la medida de lo posible, la representación paritaria de mujeres y hombres, conforme a lo establecido en el artículo 19.2 de la Ley 9/2007, de 22 de octubre, y a la definición de representación equilibrada contenida en el artículo 3.3 de la Ley 12/2007, de 26 de noviembre, para la Promoción de la Igualdad de Género en Andalucía, modificada por la Ley 9/2018, de 8 de octubre.

El Comité de Seguridad TIC podrá convocar a sus reuniones 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 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.

En particular, le corresponde:

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.

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 reevaluación periódica de los análisis de riesgos necesarios.

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

e. 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

00159863

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.

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

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

La Presidencia del Comité de Seguridad TIC ostenta la representación del Comité de 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.

00159863

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 TIC de la Consejería.

El Comité de 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 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 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 Presidencia o suplente en su caso, y de la persona que ostente la condición de Delegado de Protección de Datos o de responsable de la Unidad de Seguridad TIC.

Los miembros del Comité de 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 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 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.

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

6.3. Responsabilidad de la Consejería en relación a la estructura organizativa de la seguridad TIC y la protección de datos personales.

En el ámbito organizativo de la seguridad TIC y la protección de datos de carácter personal de la Consejería de Fomento, Infraestructuras y Ordenación del Territorio, la responsabilidad de la Información, de los Servicios, de los Sistemas, de la Seguridad TIC y de los Tratamientos de datos de carácter personal, corresponde a la Consejería, sin perjuicio de que su ejercicio se lleve a cabo por órganos o centros directivos, o personas físicas concretas, en virtud de la organización y funcionamiento interno de la propia Consejería en el ejercicio de sus competencias.

6.4. Responsables de la Información.

Los Responsables de la Información serán los órganos directivos que decidan sobre la finalidad, contenido y uso de la información.

00159863

Sus principales funciones, dentro de su ámbito de actuación y en relación con la seguridad TIC, son las siguientes:

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

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

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

6.5. Responsables de los Servicios.

Los Responsables de los Servicios serán los órganos directivos que decidan sobre las características de los servicios a prestar, cabiendo la posibilidad que puedan coincidir en la misma persona u órgano las responsabilidades de la información y del servicio.

Sus principales funciones, dentro de su ámbito de actuación y en relación con la seguridad TIC, son las siguientes:

a. Ayudar a determinar los requisitos de seguridad de los servicios a prestar, categorizando los servicios mediante la valoración de los impactos de los incidentes que puedan producirse, entre otros criterios.

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

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

6.6. Responsables de los Sistemas.

Los Responsables de los Sistemas serán las personas adscritas a la Unidad Administrativa responsable de Informática designadas al efecto por la persona titular de la jefatura del Servicio y figurarán en la documentación de seguridad de los sistemas de información. Para cada sistema de información deberá existir una persona Responsable de Sistema, siendo posible que una misma persona sea responsable de varios sistemas.

En el caso de los Sistemas que no dependan de las Unidades Administrativas responsables de Informática de la Consejería, los Responsables de los Sistemas serán las personas titulares de las unidades administrativas designadas como responsables del contrato o como director/a del expediente, salvo que se designe específicamente para ello a otra persona adscrita a los anteriores.

Sus deberes y responsabilidades serán las siguientes:

a. Realizar la implantación y mantenimiento de los controles de carácter procedimental y operacional, así como de las medidas técnicas de protección de los datos, aplicaciones y sistemas de información en los términos previstos en el Anexo II del 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, y en la presente política de seguridad.

b. Velar en su ámbito correspondiente, por el cumplimiento de los términos previstos en la política de seguridad TIC de la Junta de Andalucía, en la política de seguridad de las TIC y de la protección de datos de carácter personal de la Consejería y en todo su desarrollo normativo.

c. Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.

d. Definir la topología y forma de gestión de los sistemas de información estableciendo los criterios de uso y los servicios disponibles en el mismo.

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

00159863

f. Ejecutar la suspensión acordada del manejo de una cierta información o de la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Con carácter previo, la decisión de suspensión debe ser acordada por las personas Responsables de la Información afectada, del Servicio afectado y la Unidad de Seguridad TIC, antes de ser ejecutada.

g. Realizar las tareas adicionales previstas para el Responsable del Sistema en el Anexo A de la guía CCN-STIC-801 del Esquema Nacional de Seguridad.

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

6.7. Responsable de Seguridad TIC: la 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 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.

6.8. Responsables de los tratamientos de datos de carácter personal.

Sin perjuicio de lo señalado en el apartado 6.3, los Responsables de los Tratamientos de datos de carácter personal de la Consejería serán los órganos directivos que

00159863

determinen los fines y medios de los tratamientos, de conformidad con el artículo 4.7 del Reglamento General de Protección de Datos.

Con carácter general, en la Consejería, los Responsables de la Información, es decir, los órganos directivos, tendrán la condición de Responsables del Tratamiento respecto a los tratamientos sobre los que determinen sus fines y medios, salvo que las normas aplicables sobre asignación de atribuciones en materia de protección de datos de carácter personal dispongan otra cosa.

6.9. Encargados de tratamientos de datos personales.

Sus principales funciones y responsabilidades son las establecidas en el Reglamento General de Protección de Datos y normativa aplicable, dentro de su ámbito de actuación.

Cuando se vaya a realizar un tratamiento de datos de carácter personal por cuenta de un Responsable del Tratamiento, este elegirá únicamente un Encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del Reglamento General de Protección de Datos y garantice la protección de los derechos del interesado, de conformidad con el artículo 28 del Reglamento General de Protección de Datos.

Cuando el encargado del tratamiento preste su servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Consejería y se ajustarán al Esquema Nacional de Seguridad.

El encargado del tratamiento no recurrirá a otro encargado sin la autorización previa por escrito, específica o general, del responsable. En este último caso, el encargado informará al responsable de cualquier cambio previsto en la incorporación o sustitución de otros encargados, dando así al responsable la oportunidad de oponerse a dichos cambios.

6.10. Delegado de Protección de Datos (DPD) de la Consejería.

En la Consejería de Fomento, Infraestructuras y Ordenación del Territorio existirá una persona que ostente la condición de Delegado de Protección de Datos, a efectos de lo establecido en los artículos 37 y 38 del Reglamento General de Protección de Datos.

La persona que ostente la condición de Delegado de Protección de Datos será designada por la persona titular de la Secretaría General Técnica entre personal funcionario adscrito a la Consejería, no pudiendo ser removida ni sancionada por el desempeño de sus funciones, salvo que incurriera en dolo o negligencia grave en su ejercicio.

La persona que ostente la condición de Delegado de Protección de Datos podrá poner en conocimiento del Comité de Seguridad TIC las cuestiones relacionadas con la protección de datos que sea necesario y participará, desde el inicio, en todas las cuestiones relacionadas con la protección de datos, contribuyendo así al cumplimiento de la protección de datos personales desde el diseño y por defecto.

Son funciones de la persona que ostente la condición de Delegado de Protección de Datos, entre las demás que le corresponden de conformidad con el artículo 39 del Reglamento General de Protección de Datos y demás normativa de aplicación, las siguientes:

a. Informar y asesorar al Responsable o al Encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del Reglamento General de Protección de Datos y de cuantas disposiciones de protección de datos sean de aplicación.

Destacan en este apartado, el asesoramiento en materia de protección de datos a Responsables de Tratamientos en la confección de los modelos de formularios de recogida de datos personales, el asesoramiento a Responsables de Tratamientos sobre la oportunidad y modo de informar a las personas interesadas y afectadas por violaciones de la seguridad de sus datos personales que entrañen un alto riesgo para los derechos y libertades de las personas físicas, o el asesoramiento sobre la oportunidad y modo de

00159863

notificar los incidentes de seguridad sobre datos de carácter personal a la autoridad de control correspondiente en dicha materia.

b. Supervisar el cumplimiento de lo dispuesto en el Reglamento General de Protección de Datos, y de cuantas disposiciones de protección de datos sean de aplicación, así como de las políticas del Responsable o del Encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.

c. Supervisar la gestión del registro de actividades de tratamiento de los Responsables de Tratamiento de la Consejería, debiendo éstos facilitarle la información necesaria para ello.

d. Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35 del Reglamento General de Protección de Datos.

e. Cooperar con la Autoridad de Control.

f. Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36 del Reglamento General de Protección de Datos y realizar consultas, en su caso, sobre cualquier otro asunto.

El Delegado de Protección de Datos deberá ser consultado por parte del órgano directivo proponente de la Consejería acerca de todo proyecto de carácter técnico, normativo, o de contratación administrativa que se inicie y del que pueda derivarse en el futuro un tratamiento de datos de carácter personal. Dicho órgano directivo deberá determinar, de manera motivada, si del proyecto en cuestión se podrá derivar un tratamiento de datos de carácter personal, y en el caso de que así sea, deberá someterlo a consulta del Delegado de Protección de Datos.

El Delegado de Protección de Datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

6.11. Resolución de conflictos.

En caso de conflicto entre los diferentes responsables, éste será resuelto por el órgano superior jerárquico común. En su defecto, prevalecerá la decisión del Comité de Seguridad TIC de la Consejería.

En los conflictos entre las personas responsables que componen la estructura organizativa de la presente política de seguridad en los que se vean afectados tratamientos de datos de carácter personal, prevalecerá la decisión que presente un mayor nivel de exigencia respecto a la protección de los mismos.

6.12. Cooperación con otros órganos y otras Administraciones en materia de 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 de la información, se fomentará el establecimiento de mecanismos de comunicación con otros agentes especializados en esta materia. En especial, se contemplarán los siguientes:

- Comité de Seguridad TIC de la Junta de Andalucía.
- 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.
- 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

00159863

acciones relacionadas con la delincuencia informática y los fraudes en el sector de las telecomunicaciones.

7. Enfoque técnico de referencia de la seguridad TIC y de la protección de datos de carácter personal de la Consejería.

7.1. Esquema Nacional de Seguridad.

Como regla general, la Consejería de Fomento, Infraestructuras y Ordenación del Territorio adoptará el Esquema Nacional de Seguridad como enfoque técnico de referencia de la seguridad TIC y de la protección de datos de carácter personal, sin perjuicio de la obligación de uso de otros enfoques técnicos que, en estas materias, establezca la normativa vigente.

Por tanto, en el ámbito de la protección de datos de carácter personal de la Consejería, la aplicación de las medidas de seguridad también estará marcada por los criterios establecidos en el Esquema Nacional de Seguridad y este esquema en la Consejería, no sólo será de aplicación a sistemas relacionados con el ejercicio de derechos o con el cumplimiento de deberes por medios electrónicos, o con el acceso por medios electrónicos de los ciudadanos para recabar información y estado del procedimiento administrativo, sino que se extenderá a todo el ámbito de la seguridad TIC y la protección de datos personales.

7.2. Inventario, clasificación y control de activos TIC.

Los activos TIC se encontrarán inventariados, debiendo ser asignadas las responsabilidades para su recopilación, custodia y mantenimiento actualizado.

Los activos TIC se clasificarán de acuerdo a distintos criterios que permitan facilitar la determinación de las medidas de seguridad más adecuadas para su protección.

7.3. Registro de actividades de tratamiento de datos de carácter personal.

De acuerdo con lo establecido en el artículo 30 del Reglamento General de Protección de Datos, cada Responsable de Tratamiento y, en su caso, su representante llevarán un registro de las actividades de tratamiento efectuadas bajo su responsabilidad y cada Encargado de Tratamiento y, en su caso, el representante del Encargado, llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un Responsable.

7.4. Gestión de riesgos.

El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado.

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.

Las medidas de seguridad se reevaluarán y actualizarán periódicamente, para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección, llegando incluso a un replanteamiento de la seguridad, si fuese necesario.

La responsabilidad de la valoración de la información y de los servicios para la categorización de los sistemas es de los Responsables de Información y de Servicios correspondientes. Los Responsables de la Información y de los Servicios son los responsables de aceptar los riesgos residuales calculados en el análisis sobre la información y los servicios, respectivamente, y de realizar su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea. El Comité de Seguridad TIC es responsable de realizar un seguimiento de los principales riesgos residuales asumidos por la organización y de aprobar posibles actuaciones respecto de ellos.

En caso de tratamientos de datos personales, teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos

00159863

y libertades de las personas físicas, el Responsable y el Encargado del Tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.

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

Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el Responsable del Tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.

El Responsable del Tratamiento recabará el asesoramiento del Delegado de Protección de Datos al realizar la evaluación de impacto relativa a la protección de datos.

En caso necesario, el Responsable examinará si el tratamiento es conforme con la evaluación de impacto relativa a la protección de datos, al menos cuando exista un cambio del riesgo que representen las operaciones de tratamiento.

Una vez determinadas las valoraciones de los diferentes tipos de información que se manejan y los diferentes servicios que se prestan, la Unidad de Seguridad TIC, de acuerdo a los niveles máximos de cada dimensión de seguridad y por tanto de la categoría del sistema, determinará el conjunto mínimo de medidas de seguridad que son de aplicación en el sistema.

La selección de las medidas de seguridad a aplicar será propuesta por la Unidad de Seguridad TIC al Comité de Seguridad TIC, así como el seguimiento de su aplicación.

El proceso de gestión de riesgos comprende las fases de 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. Este análisis deberá revisarse al menos con periodicidad anual por parte de la Unidad de Seguridad TIC, que elevará un informe al Comité de Seguridad TIC.

7.5. Gestión de incidentes relacionados con la seguridad TIC y la protección de datos de carácter personal.

La Consejería de Fomento, Infraestructuras y Ordenación del Territorio deberá estar preparada para la prevención, detección, reacción y recuperación de incidentes relacionados con la seguridad TIC y la protección de datos de carácter personal, tomando el Esquema Nacional de Seguridad como enfoque técnico de referencia.

El Comité de Seguridad 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.

A efectos de una mejor coordinación en materia de detección y respuesta a incidentes de seguridad TIC, la Consejería de Fomento, Infraestructuras y Ordenación del Territorio se encuentra integrada en el grupo atendido de AndalucíaCERT, conforme a la Resolución de 26 de enero de 2018, de la Dirección General de Telecomunicaciones y Sociedad de la Información, por la que se establecen normas sobre integración en el Centro de Seguridad TIC AndalucíaCERT.

Se deberán establecer procedimientos en la Consejería que definan las vías de comunicación y notificación, roles y tareas asociadas a la respuesta a incidentes de seguridad TIC y de protección de datos personales, debiendo además mantener un registro de dichos incidentes y tareas realizadas para su gestión.

00159863

Para la comunicación obligatoria de incidentes de seguridad a autoridades de control que sea requerida por otras normativas como la de protección de datos personales, o la protección de infraestructuras críticas, mientras no se desarrollen directrices específicas en el ámbito de la Junta de Andalucía, la Consejería utilizará los canales que establezcan las correspondientes autoridades de control.

En caso de violación de la seguridad de los datos personales, se actuará de acuerdo a lo dispuesto a este respecto en la normativa vigente en materia de protección de datos de carácter personal.

La Consejería realizará acciones de concienciación entre su personal abarcando, al menos, las responsabilidades que la normativa asigna en materia de seguridad y protección de datos, los conceptos básicos sobre incidentes de seguridad y los mecanismos de notificación interna.

La Consejería atenderá las consultas y peticiones que se realicen desde AndalucíaCERT para el diagnóstico, triaje y evaluación de peligrosidad e impacto de incidentes y vulnerabilidades.

En caso de que se considere que un incidente pueda ser constitutivo de delito, y proceda por tanto interponer denuncia policial, la Consejería seguirá el protocolo de actuación que determinen los centros directivos con atribuciones al respecto.

7.6. Auditorías de seguridad TIC y de protección de datos personales.

Los sistemas de información serán objeto de una auditoría regular ordinaria, al menos cada dos años, que verifique el cumplimiento de los requerimientos del Esquema Nacional de Seguridad. Estas auditorías ordinarias así como las extraordinarias se harán de acuerdo con lo establecido en el art. 34 del Real Decreto 3/2010, de 8 de enero, y la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información, aprobada por Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública.

La Unidad de Seguridad TIC se encargará del diseño y ejecución de los programas de actuación para las auditorías de cumplimiento que correspondan, mientras que el Delegado de Protección de Datos supervisará el cumplimiento de las auditorías correspondientes en materia de protección de datos.

Con el fin de optimizar la utilización de los recursos públicos y garantizar una mejor coordinación entre la seguridad TIC y la protección de datos personales, en relación a las auditorías de seguridad de sistemas de información y las auditorías de protección de datos personales o medidas análogas de verificación, evaluación y valoración de seguridad de los tratamientos, siempre que sea posible, se promoverá su realización interna o su encargo, de manera conjunta.

Los informes de auditoría serán presentados a la personas Responsables de la Información, Sistemas, Servicios y Tratamientos de datos personales que correspondan, así como a la persona responsable de la Unidad de Seguridad TIC y al Delegado de Protección de Datos en caso de afectación a datos de carácter personal. Estos últimos analizarán estos informes y presentarán sus conclusiones a los Responsables que correspondan para que se adopten las medidas correctoras adecuadas. Los resultados obtenidos determinarán las líneas de actuación a seguir y las posibles modificaciones a realizar sobre los controles y la normativa de seguridad. Los informes, conclusiones, y medidas correctoras propuestas se presentarán al Comité de Seguridad TIC, que aprobará las actuaciones pertinentes.

8. Desarrollo de la política de seguridad TIC y de la protección de datos de carácter personal de la Consejería.

8.1. Bases del desarrollo.

En base al artículo 2.5 de la Orden de 9 de junio de 2016, de la Consejería de Empleo, Empresa y Comercio, 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

00159863

Andalucía, la Consejería de Fomento, Infraestructuras y Ordenación del Territorio podrá ampliar y desarrollar, sobre la base de los mínimos establecidos, las resoluciones que se aprueben, en el marco regulatorio de referencia de la política de seguridad TIC y de protección de datos de la Administración de la Junta de Andalucía.

8.2. Niveles de desarrollo.

El desarrollo de la política de seguridad TIC y protección de datos de carácter personal de la Consejería, se ajustará a las exigencias establecidas en el presente documento, y se efectuará en cuatro niveles, según el ámbito de aplicación y nivel de detalle técnico, de manera que cada elemento normativo de un determinado nivel de desarrollo se fundamente en los del nivel superior.

Los cuatro niveles de desarrollo de la política son los siguientes:

• Primer nivel: Política de seguridad TIC y de la protección de datos de carácter personal. Esta política deberá ser aprobada por Orden de la Consejería.

• Segundo nivel: Planes Directores de Seguridad y normas de seguridad TIC y de protección de datos personales. Se incluyen bajo este nivel los Planes Directores de Seguridad y normas generales de seguridad TIC y protección de datos personales, que serán desarrollados con mayor detalle en los niveles inferiores. Los planes y normas de segundo nivel serán aprobadas mediante Resolución de la Viceconsejería, a propuesta del Comité de Seguridad TIC.

• Tercer nivel: Procedimientos. Describen la secuencia concreta de actividades que permiten satisfacer las obligaciones contenidas en las normas. Su aprobación corresponderá a la persona titular de la Secretaría General Técnica.

• Cuarto nivel: Procedimientos técnicos y documentación técnica o especializada. Incluye todo tipo de documentación técnica o especializada que se considere necesaria para completar el desarrollo normativo de seguridad TIC y protección de datos personales de la Consejería, en particular ofrecerán información sobre cómo actuar ante situaciones y tecnologías específicas. Será aprobada por la persona titular de la jefatura del Servicio de Informática.

La Unidad de Seguridad TIC deberá mantener la documentación de seguridad actualizada y organizada, mientras que el Comité de Seguridad TIC establecerá los mecanismos necesarios para compartir la documentación derivada del desarrollo normativo con el propósito de normalizarlo, en la medida de lo posible, en todo el ámbito de aplicación de la política.

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 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 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 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 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.

00159863

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 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 TIC, 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 la política de seguridad TIC o de la normativa de seguridad derivada.

9.3. Formación y concienciación

La Consejería desarrollará actividades de formación y concienciación en materias 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.

10. Actualización y difusión de la política de seguridad.

La política de seguridad TIC y de la protección de datos de carácter personal de la Consejería, deberá estar en proceso de revisión permanente, a fin de mantenerla actualizada y adecuada a sus objetivos.

Las modificaciones de la política de seguridad se realizarán a propuesta del Comité de Seguridad TIC, y serán aprobadas por la persona titular de la Consejería de Fomento, Infraestructuras y Ordenación del Territorio.

A los efectos de su mejor difusión entre el personal de la organización y de otras partes interesadas, la presente política de seguridad 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 TIC de la Consejería.

Los medios de difusión del desarrollo normativo de la política de seguridad se establecerán, en su caso, por el Comité de Seguridad TIC de la Consejería.

00159863