3. Otras disposiciones

CONSEJERÍA DE ECONOMÍA, CONOCIMIENTO, EMPRESAS Y UNIVERSIDAD

Orden de 12 de julio de 2019, por la que se establece la política de seguridad de las tecnologías de la información y comunicaciones en el ámbito de la Consejería y de sus entidades adscritas.

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 solo 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, las personas profesionales y las empresas, como a las Administraciones Públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

La Consejería de Economía, Conocimiento, Empresas y Universidad depende de los sistemas de las tecnologías de la información y comunicaciones (en adelante, sistemas TIC) para alcanzar sus objetivos en el ámbito de su competencia con la calidad necesaria. Por ello, estos sistemas deben ser administrados con diligencia, adoptando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o de los servicios prestados.

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, su 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.

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 a los mismos.

Por otro lado, la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y la Ley 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 aquéllas entre sí.

En concreto, la Ley 39/2015, de 1 de octubre, tiene como uno de sus objetivos centrales regular las relaciones entre las Administraciones, la ciudadanía y las empresas, teniendo

00159406

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

Para el desarrollo de esta política de seguridad de las tecnologías de la información y las comunicaciones se ha seguido lo indicado en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de Protección de Datos) (en adelante, RGPD), así como en la legislación estatal vigente en materia de protección de datos personales; en 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 (en adelante, ENS) y su modificación parcial mediante Real Decreto 951/2015, de 23 de octubre; en el Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía; y en 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 Andalucía.

En la elaboración de esta política de seguridad, asimismo, se ha tenido en cuenta el contexto de la administración electrónica y 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.

Esta política de seguridad establece el compromiso de la Consejería de Economía, Conocimiento, Empresas y Universidad con la seguridad de los sistemas de información, define los objetivos y criterios básicos para el tratamiento de la misma, concreta el contenido de ese marco normativo de seguridad en esta Consejería y la estructura organizativa y de gestión que velará por su cumplimiento.

Pretende, en definitiva, dirigir y dar soporte a la gestión de la seguridad de la información mediante el establecimiento de una estructura organizativa en la que se apoyará el gobierno de la seguridad, así como dotarse de unas directrices básicas de acuerdo con los requisitos propios de seguridad y con la regulación aplicable, constituyéndose en el marco dentro del que se definirá el conjunto de normas reguladoras, procedimientos y prácticas que determinen el modo en que los activos son gestionados, protegidos y distribuidos.

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

En la elaboración y tramitación de esta 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, 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 citado 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

00159406

de aplicación; acerca del de transparencia, aunque se trata de una disposición de organización interna, ha habido consulta previa con trámite de audiencia a la ciudadanía; y, por fin, es eficiente porque no solo 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.

En su virtud, a propuesta de la Secretaría General Técnica, de acuerdo con lo dispuesto en el artículo 26.2.a) de la Ley 9/2007, de 22 de octubre, los artículos 44.2 y 46.4 de la Ley 6/2006, de 24 de octubre, de Gobierno de la Comunidad Autónoma de Andalucía, en el Decreto del Presidente 2/2019, de 21 de enero, de la Vicepresidencia y sobre reestructuración de Consejerías, y en el Decreto 104/2019, de 12 de febrero, por el que se regula la estructura orgánica de la Consejería de Economía, Conocimiento, Empresas y Universidad,

D I S P O N G O

CAPÍTULO I

Disposiciones generales

Artículo 1. Objeto.

1. De conformidad con lo establecido en el artículo 11 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, la presente Orden tiene por objeto definir y regular la política de seguridad de las tecnologías de la información y comunicaciones (en adelante, TIC) de la Consejería de Economía, Conocimiento, Empresas y Universidad, que se ha de aplicar en el tratamiento de los activos TIC de su titularidad o cuya gestión tenga encomendada.

2. La presente orden constituye el documento de política de seguridad TIC de la Consejería de Economía, Conocimiento, Empresas y Universidad.

Artículo 2. Misión y objetivos de la Consejería de Economía, Conocimiento, Empresas y Universidad.

De conformidad con el Real Decreto 3/2010, de 8 de enero, y de acuerdo con la guía de seguridad CCN-STIC-805, en la que se indica que en la política de seguridad TIC se hará referencia a la misión del organismo, le corresponden a la Consejería de Economía, Conocimiento, Empresas y Universidad las competencias atribuidas en el artículo 1 del Decreto 104/2019, de 12 de febrero, por el que se regula su estructura orgánica.

Artículo 3. Ámbito de aplicación.

1. De acuerdo con lo dispuesto en el artículo 10.3 del Decreto 70/2017, de 6 de junio, por el que se modifica el Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad TIC en la Administración de la Junta de Andalucía, la política de seguridad TIC de la Consejería de Economía, Conocimiento, Empresas y Universidad y sus documentos complementarios serán de aplicación, además de a sus órganos directivos centrales y periféricos, a las entidades vinculadas o dependientes que se encuentren adscritas orgánicamente a la misma.

2. También será de aplicación para todo el personal que acceda tanto a los sistemas de información como a la propia información, ya sea en formato electrónico o en papel, que sea gestionada por la Consejería de Economía, Conocimiento, Empresas y Universidad, con independencia de cuál sea el destino, adscripción o relación con la misma.

00159406

Artículo 4. Marco regulador.

1. Se asume como marco regulador de la seguridad TIC el que en cada momento se defina, en virtud de la disposición adicional primera del Decreto 1/2011, de 11 enero, por la Consejería competente en materia de coordinación y ejecución de las políticas de seguridad de los sistemas de información y telecomunicaciones, a propuesta del Comité de Seguridad TIC de la Junta de Andalucía. Todo ello, sin perjuicio de otra normativa aplicable a la Consejería de Economía, Conocimiento, Empresas y Universidad en virtud de su naturaleza legal y de sus competencias.

2. La Consejería de Economía, Conocimiento, Empresas y Universidad podrá ampliar y desarrollar el marco regulador de la seguridad TIC en los términos previstos en el artículo 29, teniendo en cuenta lo previsto en la disposición adicional 1.ª 1.a) del Decreto 1/2011, de 11 de enero.

Artículo 5. Objetivos, principios y definiciones.

En el ámbito de la presente orden se aplicarán las definiciones, objetivos y principios establecidos, respectivamente, en los artículos 2, 4 y 5 del Decreto 1/2011, de 11 de enero.

CAPÍTULO II

Política de seguridad TIC

Artículo 6. Contexto.

La seguridad de la información implica prácticamente a todas las áreas de la Consejería de Economía, Conocimiento, Empresas y Universidad, habida cuenta de que ha de estar presente en todos los ámbitos de su actividad y debe tener un carácter multidisciplinar, abarcando áreas como la informática y comunicaciones, gestión de personal y financiera o ejecución de proyectos.

Artículo 7. Obligaciones generales.

1. Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para afectar a la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que las unidades organizativas, entendiéndose por tal órganos y unidades administrativas, deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad (en adelante, ENS) y por la legislación de protección de datos de carácter personal, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

2. Las diferentes unidades organizativas deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Así, los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos TIC. Las unidades organizativas deben estar preparadas para prevenir, detectar, responder y recuperarse de los incidentes de seguridad, de acuerdo con lo previsto en los artículos 8, 9, 10 y 11.

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

00159406

4. Las reglas de uso de los recursos TIC serán trasladadas convenientemente, en la medida en que pueda resultar necesario o recomendable, al clausulado de los contratos suscritos por la Consejería de Economía, Conocimiento, Empresas y Universidad y a los demás instrumentos jurídicos en lo que se vertebre cualquier prestación de servicios TIC a la misma.

5. Toda la documentación generada para el desarrollo de proyectos TIC tendrá la obligación de utilización de un lenguaje no sexista.

Artículo 8. Prevención.

1. Las unidades organizativas deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello, deben implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos que cumpla los requisitos del ENS y del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de Protección de Datos) (en adelante, RGPD).

2. Los controles, los perfiles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

3. Para garantizar el cumplimiento de la política, las unidades organizativas deben:

a) Autorizar la puesta en funcionamiento de los sistemas TIC de su competencia.

b) Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.

c) Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

Artículo 9. Detección.

1. Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple ralentización hasta su detención, se deberán monitorizar de manera continua para detectar anomalías en los niveles de prestación de los mismos y actuar en consecuencia según lo establecido en el ENS.

2. La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con lo dispuesto en el ENS. Así, se establecerán mecanismos de detección, análisis y reporte que lleguen a las personas responsables tanto de una manera regular, como cuando se produzca alguna desviación significativa de los parámetros que se hayan preestablecido como normales.

Artículo 10. Respuesta.

Las unidades organizativas deben:

a) Colaborar con el equipo de gestión de incidentes de seguridad de la Consejería de Economía, Conocimiento, Empresas y Universidad.

b) Designar un punto de contacto para las comunicaciones relativas a incidentes detectados en otras unidades organizativas o en otros organismos.

c) Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta ante Emergencias Informáticas.

Artículo 11. Recuperación.

Para garantizar la disponibilidad de los servicios críticos, las unidades organizativas deben colaborar en el desarrollo de planes de continuidad de sus sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación liderados por el Comité de Seguridad TIC.

00159406

Artículo 12. Estructura organizativa de la seguridad TIC.

1. La gestión de la seguridad de la información va íntimamente ligada al establecimiento de una organización de seguridad. Dicha organización se establece mediante la identificación de las diferentes actividades y responsabilidades en materia de gestión de la seguridad y mediante su asignación formal a los agentes que correspondan, con arreglo al principio de básico de función diferenciada recogido tanto en el ENS como en la política de seguridad TIC de la Junta de Andalucía.

2. Atendiendo a dicho principio, la estructura que se define en este documento diferencia tres bloques de responsabilidad:

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

b) El desarrollo y/o explotación del sistema de información.

c) La función de supervisión de la seguridad del sistema de información.

En este sentido, los distintos bloques de responsabilidad mencionados quedarán distribuidos convenientemente, conforme a lo estipulado en el artículo siguiente, sobre los distintos agentes integrantes de la siguiente estructura organizativa en dos niveles:

a) En la Consejería de Economía, Conocimiento, Empresas y Universidad:

1.º El Comité de Seguridad TIC.
2.º Las personas responsables de la información.
3.º Las personas responsables del servicio.
4.º La Unidad de Seguridad TIC.
5.º La persona responsable de seguridad TIC.
6.º Las personas responsables del sistema.

Además, de conformidad con lo establecido en la normativa sobre protección de datos de carácter personal, deberán existir las siguientes figuras que ostentan funciones directamente relacionadas con la seguridad TIC:

7.º La persona delegada de protección de datos.
8.º La persona responsable del tratamiento de datos de carácter personal.
9.º La persona encargada del tratamiento de datos de carácter personal.

b) En cada una de las entidades vinculadas o dependientes:

1.º El Comité de Seguridad TIC.
2.º Las personas responsables de la información.
3.º Las personas responsables del servicio.
4.º La persona delegada de protección de datos.
5.º La persona responsable de seguridad TIC.
6.º Las personas responsables del sistema.

3. Dependiendo de las necesidades y circunstancias de la organización, en ciertos casos, la función de algunos de estos agentes podrá recaer sobre una misma persona, unidad o departamento.

4. Con sujeción al marco previsto por el ENS, por la normativa en materia de protección de datos, por la política de seguridad TIC de la Junta de Andalucía y por su normativa de desarrollo, en las entidades vinculadas o dependientes de la Consejería de Economía, Conocimiento, Empresas y Universidad, la responsabilidad de la conformación y designación de estas figuras recaerá sobre las propias entidades vinculadas o dependientes.

Artículo 13. Creación del Comité de Seguridad TIC de la Consejería de Economía, Conocimiento, Empresas y Universidad.

Se crea el Comité de Seguridad TIC de la Consejería de Economía, Conocimiento, Empresas y Universidad como órgano de los regulados en el artículo 10 del Decreto 1/2011, de 11 de enero, para la dirección y seguimiento en materia de seguridad de los activos TIC de los que dicha Consejería sea titular o cuya gestión tenga encomendada.

00159406

Artículo 14. Composición del Comité de Seguridad TIC.

1. El Comité de Seguridad TIC de la Consejería de Economía, Conocimiento, Empresas y Universidad estará compuesto por los siguientes miembros:

a) La presidencia le corresponderá a la persona titular de la Viceconsejería, la cual tendrá voto de calidad en la toma de decisiones del Comité en caso de empate.

b) La vicepresidencia, que será ejercida por la persona titular de la Secretaría General Técnica.

c) Las vocalías, que serán desempeñadas por:

1.º La persona titular de cada uno de los órganos directivos centrales de la Consejería de Economía, Conocimiento, Empresas y Universidad que tengan responsabilidad sobre algún sistema de información.

2.º La persona titular de la Coordinación General de la Secretaría General Técnica.

d) La secretaría será ejercida por la persona titular de la Jefatura del Servicio de Informática, con voz y voto.

2. La persona delegada de protección de datos y la persona responsable de seguridad TIC, en el caso de que no formen parte del Comité como vocales o ejerciendo la secretaría, asistirán en calidad de personas asesoras a las reuniones del Comité de Seguridad TIC, salvo que puntualmente se disponga lo contrario de forma expresa por parte de la presidencia.

3. La composición del Comité de Seguridad TIC, teniendo en cuenta a sus suplentes, deberá tener una representación equilibrada entre hombres y mujeres, conforme a lo establecido en los artículos 3.3 y 11.2 de la Ley 12/2007, de 26 de noviembre, para la Promoción de la Igualdad de Género en Andalucía.

Artículo 15. Suplencias en el Comité de Seguridad TIC.

En caso de vacante, ausencia, enfermedad y, en general, cuando concurra una causa justificada, la persona titular de la presidencia podrá ser sustituida por la persona titular de la vicepresidencia. La vicepresidencia y las vocalías podrán ser sustituidas por la persona suplente que la titular designe mediante acto documentado que remitirá al Comité de Seguridad TIC. La persona titular de la secretaría podrá ser sustituida por la persona funcionaria que designe la presidencia del Comité de Seguridad TIC.

Artículo 16. Funciones del Comité de Seguridad TIC.

Las funciones del Comité son las siguientes:

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

b) Definir, aprobar y realizar el seguimiento de los objetivos, iniciativas y planes estratégicos en materia de seguridad TIC, velando, en particular, por la coordinación entre diferentes planes que puedan coexistir. Además, le corresponde promover la mejora continua del sistema de gestión de la seguridad TIC.

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

d) Nombrar a las personas que formarán la Unidad de Seguridad TIC, garantizando el principio de función diferenciada.

e) Nombrar a la persona responsable de seguridad TIC.

f) Nombrar a las personas responsables del sistema.

g) Impulsar el cumplimiento de la política de seguridad TIC.

h) Atender las peticiones en materia de seguridad TIC de los centros directivos.

i) Informar regularmente a la persona titular de la Consejería de Economía, Conocimiento, Empresas y Universidad del estado de la seguridad de las TIC en su ámbito.

j) Elevar las propuestas de revisión de la política de seguridad TIC de la Consejería de Economía, Conocimiento, Empresas y Universidad, de sus directrices y sus normas de

00159406

seguridad, así como del marco normativo de seguridad TIC de la Junta de Andalucía, a los órganos competentes para su tramitación.

k) Aprobar las normas generales de seguridad TIC, además de la normativa de segundo y tercer nivel de seguridad TIC de la Consejería de Economía, Conocimiento, Empresas y Universidad.

l) Coordinar los esfuerzos de todo el equipo humano con responsabilidad en materia de seguridad TIC para asegurar que son consistentes y están alineados con la estrategia decidida, evitando duplicidades.

m) Realizar tareas de coordinación de los comités de seguridad TIC de las entidades instrumentales vinculadas o dependientes de la Consejería de Economía, Conocimiento, Empresas y Universidad.

n) Promover la formación, el entrenamiento y la concienciación de las medidas legales y organizativas relativas a la seguridad TIC entre el personal de Consejería de Economía, Conocimiento, Empresas y Universidad.

ñ) Elaborar y aprobar los requisitos de formación y cualificación de las personas administradoras, operadoras y usuarias desde el punto de vista de seguridad TIC de la Consejería de Economía, Conocimiento, Empresas y Universidad.

o) Coordinar y aprobar los planes de continuidad de la Consejería de Economía, Conocimiento, Empresas y Universidad.

p) Promover auditorías periódicas para verificar el correcto cumplimento de la política, la normativa y los procedimientos de seguridad.

q) Monitorizar los principales riesgos residuales asumidos y recomendar posibles actuaciones respecto a ellos.

r) Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto a ellos, velando, en particular, por la coordinación en la gestión de incidentes de seguridad TIC.

s) Priorizar las actuaciones en materia de seguridad TIC cuando los recursos sean limitados.

t) Velar para que la seguridad TIC se tenga en cuenta en todos los proyectos desde su especificación inicial hasta su puesta en producción, procurando la creación y utilización de servicios horizontales que reduzcan duplicidades y permitan un funcionamiento homogéneo de todos los sistemas.

u) Resolver los conflictos de competencia que se puedan suscitar entre las diferentes personas responsables de la gestión de la seguridad TIC o elevar propuesta para resolverlos, en su caso.

v) Impulsar la determinación de los niveles de seguridad de la información tratada, en la que se valorarán los impactos que tendrían los incidentes que afectarán a la seguridad de la información, todo ello con la participación de las personas responsables de la información, de la Unidad Seguridad TIC y con el asesoramiento de la persona delegada de protección de datos.

w) Impulsar los preceptivos análisis de riesgos, junto a las personas responsables de la información que correspondan, contando con la participación de la Unidad de Seguridad TIC y del asesoramiento de la persona delegada de protección de datos.

x) Coordinar la aceptación de los riesgos residuales por sus responsables correspondientes respecto de la información y servicios de su competencia, obtenidos en los análisis de riesgos realizados.

y) 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 de la persona delegada de protección de datos.

00159406

Artículo 17. Funcionamiento del Comité de Seguridad TIC.

1. El Comité de Seguridad TIC se reunirá con carácter ordinario, al menos, tres veces al año y, con carácter extraordinario, cuando lo decida la persona titular de la presidencia de oficio o a propuesta de alguno de sus personas miembros, y siempre que se produzca alguno de los siguientes supuestos:

a) Se produzcan incidencias de seguridad graves que afecten a cualquier sistema.

b) Surjan nuevas necesidades de seguridad que requieran la participación del Comité.

2. El Comité de Seguridad TIC podrá constituirse, convocar y celebrar sus sesiones, adoptar acuerdos y remitir actas, tanto de forma presencial como a distancia, salvo que su reglamento interno recoja expresa y excepcionalmente lo contrario.

3. Los miembros del Comité de Seguridad TIC podrán proponer a la presidencia, individual o colectivamente, la inclusión de asuntos en el orden del día. La propuesta deberá realizarse a través de medios electrónicos, dirigido a la presidencia con una antelación mínima de dos días a la fecha de la convocatoria.

4. A las sesiones del Comité de Seguridad TIC podrán asistir en calidad de asesoras, con voz pero sin voto, las personas que en cada caso estime pertinente la presidencia, por iniciativa propia o a propuesta de sus personas miembros, sin que, en ningún caso, pueda ocasionar coste económico.

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

Artículo 18. Perfiles de responsabilidad.

Las figuras o perfiles de responsabilidad que se describen en los siguientes epígrafes deben entenderse como un conjunto de responsabilidades y atribuciones que deben quedar adecuadamente cubiertas dentro de la organización, con los perfiles idóneos y con independencia de a qué persona concreta o conjunto de personas sean asignadas, cumpliendo, en cualquier caso, el principio de función diferenciada establecido tanto en el ENS como en la política de seguridad TIC de la Junta de Andalucía.

Artículo 19. Responsable de la información.

1. La figura de responsable de la información en lo relativo al ENS, es aquella quien tiene la información y determinará sus niveles de seguridad dentro del marco establecido en el Anexo I del Real Decreto 3/2010, del 8 de enero, siendo posible la presentación de una propuesta previa por parte del Comité de Seguridad TIC.

2. La persona en quien recaerá la figura de responsable de la información, y de acuerdo con la guía de seguridad CCN-STIC-801 que trata las responsabilidades y funciones en el ENS, será la persona titular del órgano directivo que tiene la responsabilidad última del uso que se haga de la información y, por tanto, de su protección. Coincidirá con la figura de responsable del tratamiento que se define en el artículo 4 del RGPD salvo que las normas aplicables sobre asignación de atribuciones en materia de protección de datos de carácter personal dispongan otra cosa.

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

a) Ayudar a determinar los requisitos de seguridad de la información, identificando los niveles de seguridad de dicha información mediante la valoración del impacto sobre esta de los incidentes que pudieran producirse.

b) Proporcionar la información necesaria a la Unidad de Seguridad TIC para realizar los preceptivos análisis de riesgos, con la finalidad de establecer las salvaguardas a implantar. Para ello, contará con la ayuda de la persona responsable del sistema.

00159406

c) En relación con los análisis de riesgos de los sistemas de información, aceptar los riesgos residuales de las informaciones manejadas que sean de su competencia.

4. El nombramiento o renovación de las personas responsables de la información se realizará en virtud de la presente política de seguridad TIC, y conservarán su condición mientras ostenten el cargo que haya determinado su nombramiento.

Artículo 20. Responsable del servicio.

1. La figura de responsable del servicio, en lo relativo al ENS, son los agentes que determinarán los niveles de seguridad de los servicios dentro del marco establecido en el Anexo I del Real Decreto 3/2010, del 8 de enero. La figura de responsable del servicio corresponderá a las personas titulares de cada unidad administrativa, con nivel igual o superior a jefatura de servicio.

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

a) Ayudar a determinar los requisitos de seguridad de los servicios a prestar, identificando los niveles de seguridad de los mismos mediante la valoración del impacto sobre éstos de los incidentes que pudieran producirse.

b) En el ámbito de cada servicio, proporcionar la información necesaria a la Unidad 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 la persona responsable del sistema.

3. El nombramiento o renovación de estas figuras responsables se realiza en virtud de la presente política de seguridad TIC, conservarán su condición mientras ostenten la posesión de la titularidad de las correspondientes unidades organizativas adscritas en cada momento a los distintos servicios prestados que haya determinado dicho nombramiento.

Artículo 21. Unidad de Seguridad TIC.

1. En virtud del artículo 11.1 del Decreto 1/2011, de 11 de enero, la Consejería de Economía, Conocimiento, Empresas y Universidad contará con una Unidad de Seguridad TIC, garantizando el cumplimiento del principio de función diferenciada recogido en el artículo 5.j) de dicho decreto. A estos efectos, esta Unidad estará adscrita a la Secretaría General Técnica.

2. El nombramiento y cese de la persona responsable y aquellas que componen dicha Unidad de Seguridad TIC de la Consejería de Economía, Conocimiento, Empresas y Universidad, se llevará a cabo por el Comité de Seguridad TIC de la Consejería. El nombramiento y cese será comunicado a dichas personas afectadas.

3. La Unidad de Seguridad TIC de la Consejería de Economía, Conocimiento, Empresas y Universidad tendrá las atribuciones que establece el artículo 11.1 del Decreto 1/2011, de 11 de enero, que se indican a continuación:

a) Las labores de soporte, asesoramiento e información al Comité de Seguridad TIC, así como de ejecución de las decisiones y acuerdos adoptados por este.

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

c) La 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.

d) La supervisión sistemática de los controles de carácter procedimental, operacional y de las medidas técnicas de protección de los datos, las aplicaciones y los sistemas.

00159406

e) La 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 por parte de los Servicios o Departamentos responsables de la prestación de los servicios TIC. Antes de la puesta en producción de nuevos sistemas de información o de evolutivos de los existentes, la Unidad de Seguridad TIC deberá evaluar los aspectos de seguridad y comunicar los posibles riesgos al centro o centros directivos responsables de la información y del servicio.

f) La definición y ejecución de los programas formativos y de concienciación relacionados con las buenas prácticas de seguridad TIC, promoviendo, en el proceso de selección de las personas participantes en estos programas, la aplicación del principio de igualdad de género.

g) La coordinación, dirección y seguimiento de la actividad en materia de seguridad TIC de las entidades vinculadas o dependientes de la Consejería de Economía, Conocimiento, Empresas y Universidad.

h) La aplicación de los criterios y directrices de gestión de la seguridad TIC emanadas de la Unidad de Seguridad TIC corporativa.

i) La elaboración y mantenimiento de un inventario de servicios y sistemas, con indicación expresa de las personas u órganos que asumen, para cada uno de ellos, las figuras de responsable de la información, responsable del servicio, responsable del sistema y responsable de seguridad TIC. Dicho listado se entregará, actualizado, al Comité de Seguridad TIC correspondiente en cada una de sus reuniones, con indicación de aquellas deficiencias que se produzcan, de modo que el Comité disponga de la información completa y pueda arbitrar los mecanismos necesarios para la subsanación de aquellas.

j) Aquellas otras que le sean encomendadas por la Secretaría General Técnica, a la que estará adscrita.

4. La persona responsable de la Unidad de Seguridad TIC de la Consejería de Economía, Conocimiento, Empresas y Universidad tendrá la condición de responsable de seguridad TIC.

Artículo 22. Responsable de seguridad TIC.

1. La persona responsable de seguridad TIC será la encargada de velar por la armonización de la seguridad de la información en sus diferentes vertientes, y tendrá las siguientes funciones y responsabilidades:

a) Dirigirá la Unidad de Seguridad TIC de la Consejería de Economía, Conocimiento, Empresas y Universidad.

b) Elaborará la normativa de seguridad que se presentará al Comité de Seguridad TIC para su aprobación.

c) Será responsable de:

1.º Conocer los cambios tecnológicos que puedan afectar a los sistemas de información, pudiendo tener consecuencias para la organización. En este caso deberá alertar al Comité de Seguridad TIC y proponer las medidas oportunas.

2.º La correcta ejecución de las instrucciones emanadas del Comité de Seguridad TIC, transmitiendo dichas instrucciones directamente o a través de la Unidad de Seguridad TIC.

3.º La presentación regular de informes sobre el estado de seguridad de los servicios TIC al Comité de Seguridad TIC.

4.º La preparación de informes en caso de incidentes excepcionalmente graves y en caso de desastres.

5.º La elaboración del Análisis de Riesgos de los sistemas, análisis que será presentado al Comité de Seguridad TIC para su aprobación. Este análisis deberá actualizarse regularmente dependiendo de la criticidad del sistema.

00159406

6.º La inspección de las verificaciones regulares de seguridad aprobadas por el Comité. El resultado de estas inspecciones se presentará al Comité de Seguridad TIC para su conocimiento y aprobación. Si como resultado de la inspección aparecen incumplimientos, propondrá medidas correctoras que presentará al Comité de Seguridad TIC para su aprobación, responsabilizándose de que sean llevadas a cabo.

7.º La elaboración y seguimiento del Plan de Seguridad que será presentado al Comité de Seguridad TIC para su aprobación.

d) Determinará, para su aprobación por el Comité de Seguridad TIC, los requisitos de formación y calificación de las personas con perfiles de personas administradoras, operadoras y usuarias desde el punto de vista de la seguridad de las TIC.

2. La persona responsable de seguridad TIC deberá poseer conocimientos de la normativa vigente y estándares nacionales e internacionales en seguridad de la información y de protección de datos, y, será nombrada entre el personal funcionario de la Unidad de Seguridad TIC por el Comité de Seguridad TIC, mediante acto documentado.

Artículo 23. Responsables de seguridad TIC de las Delegaciones Territoriales.

1. Cada Delegación Territorial que se encuentre adscrita orgánicamente a la Consejería de Economía, Conocimiento, Empresas y Universidad deberá contar con una persona Responsable de seguridad TIC en su ámbito territorial, que será designada por la persona titular de la Delegación Territorial atendiendo al principio de función diferenciada indicado en el artículo 5.j) del Decreto 1/2011, de 11 de enero.

2. Las funciones estarán circunscritas a su ámbito territorial, y serán las establecidas en artículo 21.b), d), e), f), g) y h).

Artículo 24. Responsable del sistema.

1. En virtud del artículo 10.4 del Decreto 1/2011, de 11 de enero, la presente política establece que los deberes y responsabilidades de este perfil de responsabilidad serán los previstos en el ENS y la guía CCN-STIC-801 para la figura del responsable del sistema, y, su designación, nombramiento y renovación se adoptará por decisión del Comité de Seguridad TIC y se comunicará a la persona interesada.

2. Desde la perspectiva del ENS, la figura del responsable a que se refiere este artículo, respecto de los sistemas de información cuya implantación, explotación y mantenimiento se haga fuera de la Consejería de Economía, Conocimiento, Empresas y Universidad (en otros organismos de la Junta de Andalucía o en empresas externas) será nombrada o renovada por la persona responsable de la información o la persona responsable del servicio correspondiente. El nombramiento y cese, en todo caso, será comunicado a la persona afectada.

3. Las personas responsables del sistema serán nombradas por el Comité de Seguridad TIC que corresponda, y tendrá las siguientes atribuciones:

a) Gestionar el sistema durante todo su ciclo de vida, desde la especificación, la instalación, hasta el seguimiento de su funcionamiento.

b) Definir los criterios de uso y los servicios disponibles en el sistema.

c) Elaborar los procedimientos operativos de seguridad para su aprobación por la persona responsable de seguridad TIC.

d) Determinar la configuración autorizada de hardware y software a utilizar en el sistema y aprobar las modificaciones importantes de dicha configuración.

e) Implantar y controlar las medidas específicas de seguridad del sistema.

f) Elaborar, junto con la persona responsable de seguridad TIC, los planes de mejora continua de la seguridad que deberá aprobar el Comité de Seguridad TIC.

g) Elaborar planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.

00159406

h) Suspender el manejo de cierta información o la prestación de un cierto servicio si detecta deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con las personas responsables de la información afectada, del servicio afectado y la persona responsable de seguridad TIC, antes de ser ejecutada.

Artículo 25. Entidades vinculadas o dependientes.

1. De acuerdo con lo dispuesto en el artículo 10 del Decreto 1/2011, de 11 de enero, cada entidad deberá contar con un documento de política de seguridad TIC, que será aprobado por la persona titular de la entidad correspondiente y se plasmará en los términos descritos en el Real Decreto 3/2010, de 8 de enero, sin perjuicio de lo establecido en el artículo 10.3 del Decreto 1/2011, de 11 de enero, en el que se indica que el documento de política de seguridad TIC de las Consejerías y sus documentos complementarios también serán de obligado cumplimiento para sus entidades vinculadas o dependientes.

2. Cada entidad vinculada o dependiente deberá contar con un Comité de Seguridad TIC de los regulados en el artículo 10 del Decreto 1/2011, de 11 de enero, que actuará como órgano de dirección y seguimiento en materia de seguridad de los activos TIC de su titularidad o cuya gestión tenga encomendada. Las atribuciones de los Comités de Seguridad TIC de las entidades vinculadas o dependientes podrán ser asumidas por los comités de dirección existentes en dichas entidades, circunstancia que deberá ser recogida expresamente en el correspondiente documento de política de seguridad TIC.

3. El documento de política de seguridad TIC de las entidades vinculadas o dependientes, deberá recoger la composición, atribuciones y funcionamiento del Comité de Seguridad TIC y del resto de perfiles con responsabilidad en seguridad, incluyendo, en su caso, los recogidos en el Real Decreto 3/2010, de 8 de enero, definiendo, para cada uno de ellos, los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación.

4. El Comité de Seguridad TIC de la Consejería de Economía, Conocimiento, Empresas y Universidad articulará los protocolos comunes de colaboración y coordinación necesarios con los comités de sus entidades vinculadas o dependientes.

5. Las entidades vinculadas o dependientes contarán, al menos, con una persona responsable de seguridad TIC que será nombrada por el Comité de Seguridad TIC de las mismas y que tendrá las atribuciones que establece el artículo 11.2 del Decreto 1/2011, de 11 de enero.

Artículo 26. Actualización de la política de seguridad de la información.

Una de las funciones del Comité de Seguridad TIC consistirá en la revisión anual de esta política de seguridad de la información y la propuesta de revisión o mantenimiento de la misma. Las modificaciones en la política de seguridad serán aprobadas por la persona titular de la Consejería de Economía, Conocimiento, Empresas y Universidad y difundidas a través de los medios que se establezcan por el Comité de Seguridad TIC, sin perjuicio de su publicación en el Boletín Oficial de la Junta de Andalucía.

Artículo 27. Gestión de riesgos.

1. La Consejería de Economía, Conocimiento, Empresas y Universidad realizará una gestión de la seguridad basada en los riesgos, propiciando que tanto el análisis como la gestión de riesgos sean parte esencial del proceso de seguridad, que deberá ser lo más transversal posible al resto de procesos de la organización.

2. La gestión de riesgos deberá realizarse de manera continua sobre cada sistema de información, conforme a los principios de gestión de la seguridad basada en los riesgos y evaluación periódica. Dicha gestión permitirá mantener un entorno controlado, minimizando los riesgos hasta niveles aceptables, reduciendo estos niveles mediante el despliegue de medidas de seguridad, proceso para el que se establecerá un equilibrio

00159406

entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad.

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

Artículo 28. Responsabilidades en la gestión de riesgos.

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

2. El Comité de Seguridad TIC será responsable de realizar un seguimiento de los principales riesgos residuales asumidos por la organización y de recomendar posibles actuaciones respecto de ellos.

3. 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.

Artículo 29. Análisis de riesgos.

1. El análisis de riesgos se realizará, al menos, una vez al año por parte de la Unidad de Seguridad TIC, salvo cuando se produzcan los siguientes supuestos:

a) Cuando cambie la información manejada.

b) En el momento en que se modifiquen los servicios prestados.

c) En el tiempo en que ocurra un incidente grave de seguridad.

d) En caso de que se detecten vulnerabilidades graves.

e) Cuando se determine de forma motivada por el Comité de Seguridad TIC.

2. La Unidad de Seguridad TIC elevará el informe correspondiente al análisis realizado al Comité de Seguridad TIC.

3. Para realizar el análisis de riesgos se utilizarán las metodologías y las herramientas que apliquen, de acuerdo con lo establecido en el ENS.

4. Para la armonización de los análisis de riesgos, el Comité de Seguridad TIC establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad TIC propiciará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

Artículo 30. Categorización de los sistemas.

La determinación de la categoría de un sistema se realizará de acuerdo a lo que el ENS establezca al respecto.

Artículo 31. Desarrollo normativo de la política de seguridad de la información.

1. El cuerpo normativo sobre seguridad TIC es de obligado cumplimiento y se desarrollará en tres niveles, según el ámbito de aplicación y nivel de detalle técnico, de manera que cada norma de un determinado nivel de desarrollo se fundamente en las normas de nivel superior. Dichos niveles de desarrollo normativo son los siguientes:

a) Primer nivel normativo: Política de seguridad TIC, directrices y normas generales de seguridad TIC.

b) Segundo nivel normativo: Normas específicas de seguridad TIC, que desarrollan y detallan la política de seguridad TIC, centrándose en un área o aspecto determinado.

c) Tercer nivel normativo: Procedimientos, procesos, guías e instrucciones técnicas de seguridad TIC, que dan respuesta, incluyendo detalles de implementación y tecnológicos, a cómo se puede realizar una determinada tarea cumpliendo con lo expuesto en la política de seguridad TIC.

00159406

2. Además de los documentos citados en el apartado anterior, la documentación de seguridad TIC de los órganos contemplados en el ámbito de aplicación de esta norma podrá contar, bajo criterio de la Unidad de Seguridad TIC, con otros documentos de carácter no vinculante como pueden ser: recomendaciones, buenas prácticas, informes, registros, evidencias electrónicas, y otros establecidos al respecto.

3. La Unidad de Seguridad TIC, deberá mantener la documentación de seguridad actualizada y organizada, así como gestionar los mecanismos de acceso a la misma.

4. El Comité de Seguridad TIC establecerá los mecanismos necesarios para publicar y 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 de seguridad TIC.

Artículo 32. Gestión de incidentes de seguridad y de la continuidad.

1. El Comité de Seguridad TIC 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.

2. A los efectos de una mejor gestión de los incidentes, se actuará de forma coordinada con el centro especializado y orientado a la prevención, detección y respuesta a incidentes y amenazas de seguridad en el ámbito de la administración, el sector empresarial y la ciudadanía de la Comunidad Autónoma de Andalucía (en adelante, AndalucíaCERT).

3. En relación con la violación de la seguridad de los datos personales, se actuará de acuerdo con lo previsto en el artículo 39.

Artículo 33. Concienciación y formación. Obligaciones del personal.

1. La seguridad de la información afecta a todas las personas que prestan servicios en la Consejería de Economía, Conocimiento, Empresas y Universidad y a todas las actividades, de acuerdo con el principio de seguridad integral recogido en el artículo 5 del Real Decreto 4/2010, de 8 de enero. El objetivo consiste en lograr la plena conciencia de estas personas, así como la articulación de los medios necesarios para que todas las personas que intervienen en el proceso y sus responsables jerárquicos tengan una sensibilidad hacia los riesgos que pueden acaecer. Adicionalmente, las personas con responsabilidad en el uso, operación y administración de sistemas TIC deberán haber recibido formación en el manejo seguro de los sistemas, en la medida en que la necesiten para realizar sus funciones.

2. Todas las personas que presten sus servicios en la Consejería de Economía, Conocimiento, Empresas y Universidad tienen la obligación de conocer y cumplir esta política de seguridad TIC y la normativa de seguridad, siendo responsabilidad del Comité de Seguridad TIC disponer los medios necesarios para que la información llegue a los afectados.

3. Todo el personal de la Consejería de Economía, Conocimiento, Empresas y Universidad estará obligado a asistir a una sesión de concienciación en materia de seguridad TIC al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todas las personas pertenecientes a la Consejería de Economía, Conocimiento, Empresas y Universidad, en particular a aquéllas de nueva incorporación.

Artículo 34. Terceras partes.

1. Cuando la Consejería de Economía, Conocimiento, Empresas y Universidad preste servicios a otras entidades o departamentos, o maneje información de estos, se les hará partícipes de esta política de seguridad TIC, estableciéndose canales para la comunicación y coordinación de los respectivos Comités de Seguridad TIC y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

00159406

2. Cuando la Consejería de Economía, Conocimiento, Empresas y Universidad utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta política de seguridad y de la normativa de seguridad que ataña a estos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de comunicación y resolución de incidencias, así como se garantizará que el personal correspondiente a dicha tercera parte esté adecuadamente concienciado en materia de seguridad, al menos, al mismo nivel que el establecido en esta política de seguridad TIC.

3. Cuando algún aspecto de la política de seguridad TIC no pueda ser satisfecho por una tercera parte según se establece en los párrafos anteriores, la persona responsable de seguridad TIC requerirá un informe que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por la persona responsable de la información y la persona responsable del servicio afectados antes de continuar con las actuaciones.

Artículo 35. Auditorías y conformidad normativa.

1. La Consejería de Economía, Conocimiento, Empresas y Universidad manifiesta el compromiso de auditar los sistemas de información de forma periódica con objeto de revisar el cumplimiento normativo vigente.

2. Los sistemas de información de la Consejería de Economía, Conocimiento, Empresas y Universidad serán objeto, al menos, cada dos años, de una auditoría regular ordinaria interna o externa que verifique el cumplimiento de los requisitos del ENS y de cualquier otra norma que requiera la realización de auditorías periódicas. La Unidad de Seguridad TIC coordinará estas actividades de auditoría, y analizará y elevará a la persona responsable de seguridad TIC, a la persona responsable del sistema y a la persona delegada de protección de datos si las conclusiones afectan a los datos de carácter personal. La persona responsable del sistema adoptará las medidas correctoras adecuadas. Si las conclusiones requieren, a priori, un cambio normativo, deberán elevarse al Comité de Seguridad TIC para que adopte las medidas adecuadas.

3. Con carácter extraordinario deberán realizarse auditorías siempre que se produzcan modificaciones sustanciales en el sistema de información con un potencial impacto en el cumplimiento de las medidas de seguridad.

4. Los informes de auditoría quedarán a disposición de la persona titular de la Consejería y del Comité de Seguridad TIC.

Artículo 36. Cooperación con otros órganos y otras Administraciones en materia de seguridad.

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:

a) El Comité de Seguridad TIC de la Junta de Andalucía.

b) La Unidad de Seguridad TIC de la Junta de Andalucía.

c) El Consejo de Transparencia y Protección de Datos de Andalucía.

d) La 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 del Estado, la Administración autonómica y las Entidades que integran la Administración Local.

e) La Agencia Española de Protección de Datos.

f) El Instituto Nacional de Ciberseguridad.

g) El Grupo de Delitos Telemáticos de la Guardia Civil y Brigada Central de Investigación Tecnológica del Cuerpo Nacional de Policía, para la investigación de

00159406

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

Artículo 37. Resolución de conflictos.

1. En caso de conflicto entre los diferentes responsables, este será resuelto por el órgano superior jerárquico de los mismos. En defecto de lo anterior, prevalecerá la decisión del Comité de Seguridad TIC.

2. En los conflictos entre las personas responsables que componen la estructura organizativa de la política de seguridad TIC y las personas responsables definidas en virtud de la normativa de protección de datos de carácter personal prevalecerá la decisión que presente un mayor nivel de exigencia respecto a la protección de los datos de carácter personal.

Artículo 38. Difusión de la política de seguridad de la información.

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

CAPÍTULO III

Protección de datos de carácter personal

Artículo 39. Incidencia de la normativa de protección de datos de carácter personal.

1. Todos los sistemas de información de la Consejería se ajustarán a lo exigido por el RGPD, y por el resto de la normativa general o sectorial de protección de datos de carácter personal que sea de aplicación. Todos los tratamientos de datos de carácter personal, automatizados o no automatizados, se sujetarán a la citada norma cuando se encuentren dentro de su ámbito de aplicación. En dicho ámbito cada responsable del tratamiento de datos de carácter personal aplicará las medidas técnicas y organizativas apropiadas a fin de garantizar y ser capaz de demostrar que los tratamientos de datos de carácter personal son conformes con dicha normativa, de acuerdo con el principio de responsabilidad proactiva, de conformidad con el artículo 24 del RGPD.

2. Las medidas técnicas y organizativas a implantar tendrán en cuenta lo previsto en el artículo 13.h) de la Ley 39/2015, de 1 de octubre, que reconoce como derecho de toda la ciudadanía ante las Administraciones Públicas en sus relaciones con ella la protección de datos de carácter personal, y en particular a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.

3. Teniendo en cuenta el estado de la técnica, los costes de aplicación y la naturaleza, el alcance, el contexto y los fines del tratamiento de datos de carácter personal, así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, y de conformidad con el artículo 32 del RGPD, las personas responsables del tratamiento y encargadas del tratamiento en el ámbito de aplicación de esta orden, aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) La seudonimización y el cifrado de datos personales.

b) La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

c) La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.

d) Un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

00159406

Artículo 40. Evaluación de impacto.

Cuando sea probable que un tipo de tratamiento de datos personales, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, la persona responsable del tratamiento realizará, antes del mismo, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales, de conformidad con el artículo 35 del RGPD. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos análogos. Para ello, recabará el asesoramiento de la persona delegada de protección de datos.

Artículo 41. Registro de actividades de tratamiento.

1. La persona responsable del tratamiento llevará un registro de las actividades de tratamiento de datos de carácter personal efectuadas bajo su responsabilidad, de acuerdo con lo establecido en el artículo 30 del RGPD y el resto de normativa de datos de carácter personal aplicable.

2. Cada persona encargada del tratamiento llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable, de conformidad con lo previsto en aquel artículo.

3. Los responsables o encargados del tratamiento deberán comunicar a la persona Delegada de Protección de Datos, cualquier adición, modificación o exclusión en el contenido del registro en virtud de lo establecido en el artículo 31.1, párrafo tercero, de la Ley Orgánica 3/2018, de 5 de diciembre.

Artículo 42. Violación de la seguridad de los datos personales.

1. En caso de violación de la seguridad de los datos personales, la persona responsable del tratamiento la notificará a la autoridad de control competente sin dilación indebida y, con un plazo máximo de 72 horas posteriores a computar desde que haya tenido constancia de ella, salvo que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en dicho plazo máximo, esta deberá ir acompañada de la indicación de los motivos de la dilación. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida. Dicha notificación y comunicación se atendrán a lo establecido en los artículos 33 y 34 del RGPD y en el resto de la normativa de datos de carácter personal aplicable.

2. La notificación a la autoridad de control a la que se refiere el apartado anterior podrá realizarse a través del AndalucíaCERT y del Centro Criptológico Nacional, siempre que se cumplan los requisitos del RGPD, en los casos en los que así lo disponga la política de seguridad de las tecnologías de la información y comunicaciones de la Junta de Andalucía.

Artículo 43. Persona delegada de protección de datos.

1. La figura de la persona delegada de protección de datos, en los términos establecidos en el RGPD, será asumida por una persona funcionaria del grupo A1 perteneciente a la Consejería de Economía, Conocimiento, Empresas y Universidad, que deberá tener un perfil jurídico especializado, y reconocida competencia en materia de protección de datos, de conformidad con lo establecido en los artículos 37 y 38 del RGPD y los artículos 34 y 35 de la Ley Orgánica 3/2018, de 5 de diciembre. Deberá estar adscrita a una unidad organizativa con competencias y funciones de carácter horizontal a fin de poder relacionarse adecuadamente con la dirección de la organización y con las autoridades de control.

00159406

2. Su nombramiento o renovación se adoptará y comunicará, mediante acto documentado, por la persona titular de la Viceconsejería, no pudiendo ser removida ni sancionada por desempeñar sus funciones, salvo que incurriera en dolo o negligencia grave en su ejercicio.

3. Son funciones de la persona que ostente la condición de delegada de protección de datos, además de las que le corresponden de conformidad con el artículo 39 del Reglamento General de Protección de Datos, artículos 36 y 37 de la Ley Orgánica 3/2018, de 5 de diciembre, y demás normativa de aplicación, las siguientes:

a) El asesoramiento y la supervisión:

1.º De los principios relativos al tratamiento de datos, como la limitación de finalidad, minimización o exactitud de los datos.
2.º En la identificación de las bases jurídicas de los tratamientos de datos.
3.º Del diseño e implantación de medidas de información a los afectados por los tratamientos de datos, así como el asesoramiento en la confección de modelos de formularios de recogida de datos personales.
4.º Para el establecimiento de mecanismos de recepción y gestión de las solicitudes de ejercicio de derechos por parte de las personas interesadas.
5.º De la valoración de las solicitudes de ejercicio de derechos por parte de las personas interesadas.
6.º En la contratación de las personas encargadas del tratamiento, incluido el contenido de los contratos o actos jurídicos que regulen la relación responsable-persona encargada.
7.º En la identificación de los instrumentos de transferencia internacional de datos adecuados a las necesidades y características de la organización y de las razones que justifiquen la transferencia.
8.º Del diseño e implantación de políticas de protección de datos.
9.º De la auditoría de protección de datos.
10.º En el establecimiento y gestión de los registros de actividades de tratamiento.
11.º Del análisis de riesgo de los tratamientos realizados.
12.º De la implantación de las medidas de protección de datos desde el diseño y la protección de datos por defecto adecuadas a los riesgos y a la naturaleza de los tratamientos.
13.º De la implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos.
14.º En el establecimiento de procedimientos de gestión de violaciones de seguridad de los datos, incluida la evaluación del riesgo para los derechos y libertades de las personas afectadas y los procedimientos de notificación a las autoridades de supervisión y a esas personas.
15.º Sobre la determinación de la necesidad de realización de evaluaciones de impacto sobre la protección de datos.
16.º En la realización de evaluaciones de impacto sobre la protección de datos.
17.º En la implantación de programas de formación y sensibilización del personal en materia de protección de datos.

b) La valoración de la compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos.

c) El asesoramiento sobre la existencia de normativa sectorial que pueda determinar condiciones de tratamiento específicas distintas de las establecidas por la normativa general de protección de datos.

4. La persona delegada de protección de datos asesorará y supervisará la elaboración y mantenimiento del registro de actividades de tratamiento a que se refiere el artículo 30 del RGPD, y entregará un listado actualizado del citado registro al Comité de Seguridad TIC en cada una de sus reuniones, con indicación expresa de las personas u órganos que asumen las figuras de responsable del tratamiento, encargada del tratamiento y resto de

00159406

contenidos exigidos por el citado artículo, así como de las deficiencias que en su caso se produzcan, de modo que el Comité disponga de la información completa y pueda arbitrar los mecanismos necesarios para la subsanación de aquellas.

Artículo 44. Persona delegada de protección de datos en las entidades vinculadas o dependientes.

La dirección de cada entidad vinculada o dependiente deberá nombrar una persona delegada de protección de datos que se comunicará a la Agencia Española de Protección de Datos y al Comité de Seguridad TIC de la Consejería de Economía, Conocimiento, Empresas y Universidad. La persona delegada de protección de datos, que deberá estar en posesión de una titulación superior, será designada atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados de Derecho y la práctica en materia de protección de datos, de conformidad con el artículo 35 de la Ley Orgánica 3/2018, de 5 de diciembre.

Artículo 45. Responsables del tratamiento de datos de carácter personal.

1. Las personas responsables del tratamiento de datos de carácter personal en el ámbito de aplicación de esta orden son las autoridades públicas que determinen los fines y medios de los tratamientos, de conformidad con el artículo 4.7 del RGPD.

2. En el ámbito de la política de seguridad TIC de la Consejería de Economía, Conocimiento, Empresas y Universidad, las personas responsables de la información 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.

Artículo 46. Personas encargadas del tratamiento de datos de carácter personal.

1. De conformidad con el artículo 28 del RGPD, cuando se vayan a tratar datos de carácter personal por cuenta de un responsable, este elegirá únicamente los encargados del tratamiento que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, y garantice la protección de los derechos de las personas interesadas.

2. Las principales funciones y responsabilidades, dentro de su ámbito de actuación, son las establecidas en el artículo 28 del RGPD y demás normativa de aplicación.

3. El encargado del tratamiento, y cualquier persona que actúe bajo la autoridad de la persona responsable o encargada del tratamiento, y tenga acceso a datos personales, solo podrán tratar dichos datos siguiendo instrucciones del responsable, a no ser que estén obligados a ello en virtud de normativa aplicable.

Disposición adicional única. Constitución del Comité de Seguridad TIC.

La primera reunión del Comité de Seguridad TIC tendrá por objeto la constitución, renovación o confirmación del mismo y se celebrará en un plazo máximo de un mes a partir de la entrada en vigor de la presente orden.

Disposición derogatoria única. Derogación de normas.

Quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo establecido en la presente orden y, en particular, la Orden de 10 de enero de 2017, de la Consejería de Economía y Conocimiento, por la que se regula la composición, atribuciones, funcionamiento y método de trabajo del Comité de Seguridad de las Tecnologías de la Información y Comunicaciones de dicha Consejería.

00159406

Disposición final primera. Habilitación para ejecución y desarrollo.

1. De conformidad con la presente orden, la persona titular de la Consejería de Economía, Conocimiento, Empresas y Universidad podrá ampliar y desarrollar, sobre la base de los mínimos establecidos, sus propias normas en materia de seguridad TIC, en virtud del artículo 2.5 de la Orden de 9 de junio de 2016, de la Consejería de Empleo, Empresa y Comercio, por la que se efectúa el desarrollo de la política de seguridad TIC en la Administración de la Junta de Andalucía.

2. Se habilita a la persona titular de Secretaría General Técnica para dictar cuantas actuaciones sean necesarias para la ejecución y desarrollo de lo establecido en la presente orden, en todo aquello que no esté expresamente previsto en el apartado anterior.

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, 12 de julio de 2019

ROGELIO VELASCO PÉREZ
Consejero de Economía, Conocimiento,
Empresas y Universidad

00159406