1. Disposiciones generales

CONSEJERÍA DE HACIENDA, INDUSTRIA Y ENERGÍA

Orden de 21 de octubre de 2019, por la que se establece la política de seguridad de la información de la Consejería.

ORDEN DE LA CONSEJERÍA DE HACIENDA, INDUSTRIA Y ENERGÍA, DE 21 DE OCTUBRE DE 2019, POR LA QUE SE ESTABLECE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA CONSEJERÍA

ÍNDICE

Crear las condiciones necesarias para generar confianza en el uso de los medios electrónicos en todos los ámbitos de la gestión pública, exige el establecimiento de un conjunto de procedimientos y prácticas que conviertan en una actividad integral el tratamiento y gestión de la seguridad de la información. Tal gestión es un proceso que requiere coordinar recursos humanos, medios electrónicos, normativa, procedimientos y

00164190

buenas prácticas, en el cual no caben actuaciones puntuales o tratamientos coyunturales, ya que la debilidad de un sistema la determina su punto más frágil y, a menudo, este punto es la coordinación entre medidas individualmente adecuadas, pero deficientemente ensambladas.

La Consejería de Hacienda, Industria y Energía, en adelante la Consejería, va a dar continuidad y ampliar el conjunto de actuaciones iniciados en anteriores legislaturas, y dirigidas a establecer un sistema de gestión de la seguridad de la información ajustado tanto a los marcos metodológicos vigentes, fundamentalmente MAGERIT e ISO/IEC 27001 y 27002, como a los normativos, dictados por 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, la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales; todo ello con el fin de abordar los aspectos de seguridad necesarios para la protección de sus sistemas de información, así como de las infraestructuras necesarias para el funcionamiento de estos.

La entrada en vigor del Reglamento general de protección de datos, aplicable a partir del 25 de mayo de 2018, la más reciente entrada en vigor de la Ley Orgánica 3/2018, de 5 de diciembre, así como lo dispuesto 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, hacen necesario un cambio en la organización corporativa de la seguridad de la información y los datos, creando nuevas estructuras y perfiles con responsabilidad en la seguridad tal y como se establecen en estas normas.

Por lo tanto, es necesario establecer la estructura organizativa recogida en el Decreto 1/2011, de 11 de enero, que da respuesta a las obligaciones impuestas por el Esquema Nacional de Seguridad. En concreto, este Decreto indica que cada Consejería, y entidad incluida en el ámbito de aplicación, deberá contar con un Comité de Seguridad TIC, estableciendo los mecanismos para la designación de la Unidad de Seguridad TIC, de Responsable de Seguridad y Responsables de la Información, Servicios y Sistemas; por otra parte, la presente Orden recoge las figuras que aparecen en el Reglamento general de protección de datos y en la Ley Orgánica 3/2018, de 5 de diciembre, entre las que destaca la figura de Delegado de Protección de Datos, sin olvidar a las de Responsables y Encargados del Tratamiento.

En otro orden de cosas, para formalizar los objetivos de seguridad de la Consejería resulta necesario seguir desarrollando una política que recoja las directrices básicas y duraderas de gestión de la seguridad de la información, tal y como viene descrito en el artículo 1 del Real Decreto 3/2010, de 8 de enero. La presente política está en consonancia con el Decreto 1/2011, de 11 de enero, que establece en su artículo 6 la organización de la seguridad TIC en las Consejerías y en sus entidades vinculadas o dependientes, y en su artículo 10 la obligatoriedad de que las Consejerías dispongan de su propio documento de política de seguridad TIC.

Asimismo, la presente política no debe olvidar que los objetivos de la seguridad deben estar alineados con la Resolución de 27 de septiembre de 2004, de la Secretaría General para la Administración Pública, por la que se establece el manual 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. También debe alinearse con recomendaciones y buenas prácticas, que sin ser específicamente relativas a seguridad de la información,

00164190

contribuyen a la mejora de la misma. En tal sentido se podría hablar del puesto de trabajo despejado, custodia de la documentación, etc.

Igualmente se deben asumir las competencias y objetivos establecidos en el Decreto 101/2019, de 12 de febrero, por el que se regula la estructura orgánica de la Consejería de Hacienda, Industria y Energía.

Una vez establecida la política de seguridad de la información se reforzará el correspondiente proceso de desarrollo de normas técnicas, que incluirá, entre otras, normas relativas a seguridad física, seguridad lógica, seguridad relativa al personal, gestión de autorizaciones, seguridad documental, etc.

A la vista de lo expuesto, resulta necesario establecer una estructura organizativa apropiada que facilite y ordene el trabajo en este ámbito, así como aprobar y dar a conocer a todos los colectivos implicados en la gestión y utilización de los sistemas de información de la Consejería el conjunto de medidas adoptadas y establecer los mecanismos para el seguimiento y la mejora de los procedimientos establecidos.

La presente orden se adecua a los principios de buena regulación referidos en el artículo 129 de la Ley 39/2015, de 1 de octubre. Es el instrumento legalmente determinado a través del cual la Consejería se ajustará a la normativa relativa a la seguridad de la información y los activos de tecnologías de la información y comunicaciones, creando condiciones que redundan en la creación de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, lo que permite a los ciudadanos el ejercicio de derechos y el cumplimiento de deberes a través de estos medios en las mejores condiciones. Por todo ello se da cumplimiento a los principios de necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia y eficiencia.

En su virtud, a propuesta de la Dirección General de Transformación Digital, y en el ejercicio de las competencias que me confiere el artículo 44.2 de la Ley 6/2006, de 24 de octubre, del Gobierno de la Comunidad Autónoma de Andalucía,

D I S P O N G O

Artículo 1. Objeto.

1. La presente orden tiene por objeto definir y regular la política de seguridad de la información de la Consejería, que se ha de aplicar en el tratamiento de la información, así como de los activos de tecnologías de la información y comunicaciones de su titularidad o cuya gestión tenga encomendada.

2. La presente orden constituye el «Documento de Política de Seguridad TIC» de la Consejería, en cumplimiento de lo establecido en el artículo 10 del Decreto 1/2011, 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, sin perjuicio de la obligación de cada entidad vinculada o dependiente de la Consejería de contar con su propio documento de política de seguridad TIC.

Artículo 2. Ámbito de aplicación.

La orden será de aplicación a:

a) La Consejería, tanto en sus servicios centrales como periféricos.

b) Las entidades vinculadas o dependientes de la Consejería, de conformidad con el artículo 10.3 del Decreto 1/2011, de 11 de enero, y sin perjuicio de que dichas entidades aprueben su propia política de seguridad de la información en coherencia con la presente orden.

c) Toda persona que, no estando adscrita a la Consejería, tenga acceso a la información gestionada por la Consejería o a los sistemas de información de la misma.

00164190

Artículo 3. Definiciones, objetivos y principios.

Serán aplicables en el ámbito de esta orden las definiciones, objetivos y principios establecidos en los artículos 2, 4 y 5 del Decreto 1/2011, de 11 de enero, circunscritos al ámbito competencial de los órganos y entidades contemplados en el ámbito de aplicación de esta norma.

Artículo 4. Responsabilidad general.

1. La preservación de la seguridad de la información será considerada objetivo común de todas las personas al servicio de los órganos y entidades vinculadas o dependientes contemplados en el ámbito de aplicación de esta norma, siendo estas responsables del uso correcto de la información a la que tengan acceso, así como de los activos de tecnologías de la información y comunicaciones puestos a su disposición.

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

3. Todas las personas empleadas que se incorporen a la Consejería o a sus entidades vinculadas o dependientes, o vayan a tener acceso a datos personales tratados por esta, o a algunos de sus sistemas de información, deberán ser informadas de la política de seguridad de la información y la normativa de seguridad derivada. Dicha información será proporcionada por la persona de la que dependa jerárquicamente la persona recién incorporada o a través de los medios que se articulen en función de la vinculación por la que tenga acceso a dichos datos.

4. Las personas empleadas públicas al servicio de la Administración de la Junta de Andalucía comprendidas dentro del ámbito de esta orden deberán cumplir, además, con las instrucciones y normas que regulen el comportamiento de las personas empleadas públicas en el uso de los sistemas informáticos y redes de comunicaciones de esta.

5. Cualquier persona que actúe bajo la autoridad del Responsable o Encargado de un Tratamiento de datos personales en el ámbito de aplicación de esta orden y tenga acceso a datos personales, solo tratará dichos datos respetando las instrucciones del Responsable del Tratamiento, salvo que esté obligada a ello en virtud del ordenamiento jurídico comunitario, nacional o autonómico.

Artículo 5. Estructura organizativa de la seguridad de la información.

1. La estructura organizativa de la seguridad de la información de la Consejería de acuerdo con el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, regulado por el Real Decreto 3/2010, de 8 de enero, y del Decreto 1/2011, de 11 de enero, está compuesta por:

a) Comité de Seguridad TIC.

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

c) Responsables de la Información.

d) Responsables del Servicio.

e) Responsables del Sistema.

2. Además, en el ámbito de la Consejería, y de acuerdo con lo establecido en la normativa sobre protección de datos personales, deberán existir los siguientes perfiles:

a) El Delegado de Protección de Datos.

b) Responsables del Tratamiento.

c) Encargados del Tratamiento.

3. Cada una de las entidades vinculadas o dependientes deberá disponer de una estructura organizativa de la seguridad de la información similar a la que se describe para

00164190

la Consejería, con la salvedad de que no es necesaria la Unidad de Seguridad TIC, pero sí la figura de Responsable de Seguridad.

Artículo 6. Comité de Seguridad TIC.

1. La Consejería contará con un Comité de Seguridad TIC 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 la información y de los activos TIC, y tratamiento de datos personales de los que la Consejería sea titular o cuya gestión tenga encomendada.

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

a) Presidencia: la persona titular de la Viceconsejería.

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

c) Vocalías:

1.º La persona titular del órgano directivo que tenga asignada las competencias relacionadas con la estrategia y aplicación de las tecnologías de la información y de las comunicaciones.

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

d) Secretaría: la persona titular de la Unidad de Seguridad TIC.

3. En caso de vacante, ausencia, enfermedad u otras causas legales, la persona titular de la Presidencia será sustituida por la persona titular de la Vicepresidencia. Tanto la Vicepresidencia como las Vocalías y la Secretaría podrán designar a una persona que les sustituya, con carácter permanente y aplicando un criterio de paridad entre mujeres y hombres, de entre personal funcionario a su servicio que ocupen puestos de trabajo de nivel 28 o superior, con la excepción de la Secretaría cuya persona suplente podrá ocupar puestos de nivel inferior, sin perjuicio de que posteriormente pueda designarse a otra persona suplente. Dicha designación será comunicada a la Secretaría.

4. Quien ostente la condición de Delegado de Protección de Datos asistirá en calidad de persona asesora a las reuniones del Comité de Seguridad TIC.

5. El Comité se reunirá de forma ordinaria al menos una vez por semestre. También podrá celebrar reuniones extraordinarias, adicionales a las ordinarias, si se produjeran incidentes de seguridad graves o se produjeran conflictos que pudieran afectar gravemente a los servicios prestados por la Consejería. La evaluación de la gravedad para convocar una reunión extraordinaria la realizará la persona titular de la Vicepresidencia del Comité, que lo someterá a la Presidencia del mismo. Todas las reuniones se realizarán previa convocatoria y de las mismas se levantará acta.

6. El Comité podrá convocar, a través de la presidencia por iniciativa propia o a propuesta de alguno de sus miembros, y cuando el tratamiento de determinados temas específicos lo requiera, a personal técnico de la organización a los efectos de recibir asesoramiento especializado.

7. Serán funciones propias del Comité de Seguridad TIC, como órgano de dirección y seguimiento en materia de seguridad de los activos TIC de su titularidad o cuya gestión tenga encomendada, y dentro del marco fijado por el Decreto 1/2011, de 11 de enero:

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

b) Definir y hacer seguimiento de los objetivos, iniciativas y medidas en materia de tratamiento de datos personales y seguridad de la información.

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

d) De acuerdo con lo establecido en el artículo 11.1 del Decreto 1/2011, de 11 de enero, nombrar a la persona titular de la Unidad de Seguridad TIC de la Consejería.

00164190

e) Velar por que todos los ámbitos de responsabilidad y actuación en relación a la seguridad de la información y su tratamiento queden perfectamente definidos, conociendo los nombramientos de las personas, órganos y unidades a que hace referencia el artículo 5, y garantizando que todos y cada uno de los miembros de la estructura de seguridad definida conozcan y cumplan sus funciones y responsabilidades.

f) Elevar propuestas de revisión de la política de seguridad de la información de la Consejería, de directrices y normas de seguridad de la Consejería, o de revisión del marco normativo en materia de tratamiento de datos personales y seguridad de la información de la Administración de la Junta de Andalucía, a los órganos competentes para su reglamentaria tramitación.

g) Impulsar la aprobación de las normas sobre tratamiento de datos personales y seguridad de la información.

h) Establecer directrices y supervisar el cumplimiento de la normativa en materia de tratamiento de datos personales y seguridad de la información.

i) Supervisar el nivel de riesgo y supervisar la toma de decisiones en la respuesta a incidentes de seguridad que afecten a la información y/o a los activos TIC.

j) Coordinar a los Comités de Seguridad TIC de las entidades instrumentales vinculadas o dependientes de la Consejería.

k) Promover y fomentar la divulgación y formación en cultura de la seguridad de la información, así como la educación, entrenamiento y concienciación sobre las medidas legales y organizativas relativas al tratamiento de datos personales y a la seguridad de la información entre el personal de la Consejería.

l) Impulsar que por los Responsables de la Información se proceda a la determinación de los niveles de seguridad de la información tratada, en la que se valorarán los impactos que tendrían los incidentes que afectaran a la seguridad de la información; todo ello, con la colaboración de la Unidad de Seguridad TIC.

m) Impulsar los preceptivos análisis de riesgos, junto a los Responsables de los Servicios que correspondan, contando con la participación de la Unidad de Seguridad TIC.

n) Velar por que la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular, deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.

ñ) Velar por que el desarrollo de normas que tengan incidencia en el tratamiento de datos personales y/o en el desarrollo o explotación de sistemas de información se adecue a lo establecido en la política de seguridad de la información.

o) Dar respuesta a las consultas recibidas relativas a los conflictos que puedan aparecer entre las diferentes responsables o entre diferentes áreas de la organización en materia de seguridad de la información.

p) Coordinar las medidas técnicas y organizativas establecidas en la normativa de protección de datos personales, una vez realizados 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.

q) Impulsar las tareas para la clasificación de activos de información a que hace referencia el artículo 17.

8. El Comité aprobará, por mayoría simple de su miembros, sus propias reglas de organización, funcionamiento y adopción de acuerdos.

Artículo 7. Unidad de Seguridad TIC.

1. La Consejería contará con la Unidad de Seguridad TIC, garantizando el cumplimiento del principio de función diferenciada recogido en el artículo 5.j) del Decreto 1/2011, de 11 de enero.

2. La persona titular de la Unidad de Seguridad TIC será nombrada por el Comité de Seguridad TIC a propuesta de la persona titular del órgano directivo que tenga asignada

00164190

las competencias relacionadas con la estrategia y aplicación de las tecnologías de la información y de las comunicaciones, entre personal funcionario adscrito a la Consejería.

3. La Unidad de Seguridad TIC de la Consejería tendrá las atribuciones que establece el artículo 11 del Decreto 1/2011, de 11 de enero.

4. La persona titular de la Unidad de Seguridad TIC tendrá la condición de Responsable de Seguridad, en los términos establecidos en el Real Decreto 3/2010, de 8 de enero.

5. A fin de simplificar la estructura organizativa de la gestión de la seguridad de la Consejería, la Unidad de Seguridad TIC realizará labores de apoyo a los Responsables del Tratamiento en la realización de tareas técnicas que sean competencia de dichos responsables. Entre dichas labores se incluirá la ejecución de análisis de riesgos de protección de datos personales.

6. La Unidad de Seguridad TIC coordinará el mantenimiento del registro de actividades de tratamiento de la Consejería, consolidando la información suministrada por todos los Responsables del Tratamiento.

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

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

9. La Unidad de Seguridad TIC mantendrá un registro actualizado de las normas aplicables a la Consejería en materia de seguridad de la información y de protección de datos personales.

Artículo 8. Responsables de la información.

1. La persona titular de cada órgano directivo tendrá la condición de Responsable de la Información, según el Esquema Nacional de Seguridad, de toda información sobre la que tenga capacidad para decidir sobre su finalidad, contenido y uso.

2. Los Responsables de la Información tendrán las funciones que establece para ellas el Esquema Nacional de Seguridad. Entre otras, asumirá las siguientes:

a) Determinar los requisitos de la información, valorando la información mediante la valoración de los impactos de los incidentes que puedan producirse.

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

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

Artículo 9. Responsables del Servicio.

1. La persona titular de cada órgano directivo o una unidad administrativa con rango de Servicio, integrada en dicho órgano directivo y designada por la persona titular del mismo, tendrá la condición de Responsable del Servicio, según el Esquema Nacional de Seguridad, para aquellos servicios sobre los que decida sus características y requisitos.

2. Los Responsables de los Servicios tendrán las funciones que establece para ellas el Esquema Nacional de Seguridad. Entre otras, asumirá las siguientes:

a) Determinar los requisitos de los servicios a prestar, valorando los servicios mediante la valoración de los impactos de los incidentes que puedan producirse.

00164190

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

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

Artículo 10. Responsables del Sistema.

1. La persona titular del órgano directivo que tenga asignada las competencias relacionadas con la estrategia y aplicación de las tecnologías de la información y de las comunicaciones, o una unidad administrativa con rango de Servicio, integrada en dicho órgano directivo y designada por la persona titular del mismo, tendrá la condición de Responsable del Sistema, según el Esquema Nacional de Seguridad, de cada sistema de información cuya explotación tenga encomendada dicho órgano directivo.

2. Los Responsables de los Sistemas tendrán las funciones que establece para ellas el Esquema Nacional de Seguridad. Entre otras, asumirá las siguientes:

a) Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.

b) Velar por que la seguridad de la información esté presente en todas y cada una de las partes del ciclo de vida de los sistemas de información de los que es responsable. Especialmente deberá velar por que el desarrollo de los sistemas de información siga las directrices de seguridad establecidas de manera horizontal por la Junta de Andalucía. Para todo ello, podrá contar con el asesoramiento de la Unidad de Seguridad TIC.

c) Crear, mantener y actualizar de manera continua la documentación de seguridad de los sistemas de información, con el asesoramiento de la Unidad de Seguridad TIC.

d) Definir la topología y sistema de gestión del sistema de información estableciendo los criterios de uso y los servicios disponibles en el mismo.

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

f) En caso necesario, acordar la suspensión del manejo de determinada información o la prestación de un determinado servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los Responsables de la Información y los Servicios afectados y con el Responsable de Seguridad, antes de ser ejecutada. En caso de desacuerdo se aplicará el artículo 15 de esta orden.

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

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

Artículo 11. Delegado de Protección de Datos.

1. La Consejería contará con una persona que ostente la condición de Delegado de Protección de Datos, en los términos y con las atribuciones establecidos en el Reglamento general de protección de datos, para todos los órganos y unidades administrativas de los servicios centrales y periféricos de la Consejería.

2. La figura del Delegado de Protección de Datos de la Consejería será nombrada por la persona titular de la Viceconsejería, de entre personal funcionario adscrito a la Consejería, no pudiendo ser removida ni sancionada por desempeñar sus funciones, salvo que incurriera en dolo o negligencia grave en su ejercicio. No será de aplicación a la persona que ostente la condición de Delegado de Protección de Datos el régimen

00164190

sancionador previsto en el Título IX de la Ley Orgánica 3/2018, de 5 de diciembre. En el nombramiento deberá especificarse el alcance de su designación, que podrá alcanzar a una o varias de las entidades vinculadas o dependientes de la Consejería.

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

4. La figura del Delegado de Protección de datos tendrá las funciones que establece para ella el Reglamento general de protección de datos, la Ley Orgánica 3/2018, de 5 de diciembre, y cualquier otra normativa europea, estatal o autonómica que los desarrolle. Entre otras, asumirá las siguientes:

a) Ser consultada sobre la contratación, análisis, diseño, operación y mantenimiento de todo tratamiento realizado sobre datos personales. También debe ser consultada, con carácter preceptivo, sobre todo proyecto de norma dentro del alcance de su designación, que suponga un tratamiento de datos personales.

b) Asesorar sobre la confección de los modelos de formularios de recogida de datos personales cuando el órgano directivo competente sobre el formulario lo considere conveniente, con el objetivo de supervisar que los mismos cumplen con lo establecido en los artículos 12 y 13 del Reglamento General de Protección de Datos.

c) Asesorar sobre la evaluación de impacto relativa a la protección de datos personales, tanto en la necesidad de su realización como en su elaboración.

d) Supervisar que el contenido del Registro de Actividades de Tratamiento se corresponda con las actividades efectivamente realizadas en la Consejería, debiendo los responsables facilitarle la información necesaria para ello.

e) Asesorar a Responsables del Tratamiento sobre cómo proceder en relación a la notificación de incidentes de seguridad sobre datos personales a la autoridad de control correspondiente. También asesorará y dará apoyo a Responsables del Tratamiento sobre la necesidad y manera de informar a las personas interesadas y afectadas por violaciones de la seguridad de sus datos personales, conforme a lo establecido en el artículo 34 del Reglamento General de Protección de Datos.

Artículo 12. Responsables del Tratamiento.

1. La persona titular de cada órgano directivo tendrá la condición de Responsable del Tratamiento, según el Reglamento General de Protección de Datos, de todo tratamiento de datos personales sobre el que determine los fines y medios de tratamiento.

2. Los Responsables del Tratamiento tendrán las funciones y obligaciones establecidas en la normativa sobre protección de datos personales. Entre otras, asumirán las siguientes:

a) Ser responsable del cumplimiento de lo dispuesto en el artículo 5.1 del Reglamento general de protección de datos y ser capaz de demostrarlo, para lo cual deberá establecer y supervisar las medidas técnicas y organizativas apropiadas.

b) Resolver las solicitudes de ejercicio de los derechos recogidos en los artículos 15 a 22 del Reglamento general de protección de datos.

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

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

e) Garantizar la protección de datos personales desde el diseño y por defecto, en los términos establecidos en el artículo 25 del Reglamento general de protección de datos.

00164190

f) En caso de producirse una violación de seguridad de los datos personales, lo pondrá en conocimiento del Delegado de Protección de Datos y, en su caso, procederá a notificarlo a la autoridad de control competente, así como a las personas interesadas cuando proceda.

g) Realizar la evaluación de impacto establecida en el artículo 35 del Reglamento General de Protección de Datos, cuando sea probable que el tratamiento entrañe un alto riesgo para los derechos y libertades de las personas físicas.

h) Mantener un registro de las actividades de tratamiento efectuadas bajo su responsabilidad.

Artículo 13. Encargados del Tratamiento.

1. Los Responsables del Tratamiento podrán encargar a otros órganos, así como a otras personas físicas o jurídicas, la ejecución de actividades de tratamiento.

2. Los Encargados del Tratamiento deberán cumplir todas las obligaciones que establece la normativa de protección de datos para esta figura.

3. Los Responsables del Tratamiento deberán mantener un inventario de todos los Encargados del Tratamiento a los que han encargado la realización de actividades de tratamiento, con indicación de las actividades encomendadas. Dicho inventario formará parte del registro de actividades de tratamiento y, cuando los Encargados del Tratamiento sean personas físicas, incorporará el dato del sexo de dichas personas, en cumplimiento del artículo 10.1.a) de la Ley 12/2007, de 26 de noviembre, para la promoción de la igualdad de género en Andalucía.

Artículo 14. Entidades vinculadas o dependientes.

1. Cada una de las entidades vinculadas o dependientes de la Consejería aprobará su política de seguridad de la información, que deberá ser coherente con la política de seguridad de la información de la Consejería.

2. La política de seguridad de la información de cada entidad detallará las funciones y atribuciones de cada uno de los agentes enunciados en el artículo 5, así como el procedimiento para su designación.

Artículo 15. Resolución de conflictos.

1. Los conflictos entre las diferentes personas, unidades u órganos responsables que componen la estructura organizativa de la política de seguridad de la información serán resueltos por el superior jerárquico común, que podrá elevar consulta previa al Comité de Seguridad TIC. En caso de conflicto prevalecerán las decisiones del Comité de Seguridad TIC.

2. En los conflictos entre las personas responsables que componen la estructura organizativa de la política de seguridad de la información y las personas responsables definidas en 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 16. Gestión de riesgos.

1. La gestión de riesgos debe realizarse de manera continua sobre los tratamientos y los sistemas de información, conforme a los principios de gestión de la seguridad basada en los riesgos y reevaluación periódica.

2. Se tendrán en consideración tanto los riesgos relativos a la protección de datos personales como los riesgos relativos a los sistemas de información. Para cada tipo de riesgos se utilizarán las metodologías de análisis y gestión de riesgos que resulten más adecuadas.

3. Los Responsables de la Información y de los Servicios son responsables de establecer los requisitos de la información y los servicios en materia de seguridad y, por

00164190

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.

4. La selección de las medidas de seguridad a aplicar será propuesta por el Responsable de Seguridad al Comité de Seguridad TIC.

5. El proceso de gestión de riesgos, que comprende las fases de categorización de los sistemas, análisis de riesgos y selección de medidas de seguridad a aplicar, que deberán ser proporcionales a los riesgos y estar justificadas, deberá revisarse cada año por parte del Responsable de Seguridad, que elevará un informe al Comité de Seguridad TIC.

Artículo 17. Clasificación de activos.

Los activos de información estarán clasificados de acuerdo con su sensibilidad y criticidad para el desarrollo de la actividad de la Consejería, en función de la cual se establecerán las medidas de seguridad exigidas para su protección, todo ello de conformidad con lo establecido en el Esquema Nacional de Seguridad.

Artículo 18. Auditorías de la seguridad.

1. Al menos cada dos años se realizará una auditoría de seguridad que verifique el cumplimiento de los requerimientos de la normativa sobre protección de datos personales, así como del Esquema Nacional de Seguridad, para cada tratamiento y cada sistema de información. Estas auditorías se realizarán de conformidad con lo establecido en el Esquema Nacional de Seguridad. En el caso de sistemas de información de categoría básica, esta auditoría podrá ser sustituida por una autoevaluación en los términos establecidos en el Esquema Nacional de Seguridad.

2. Los informes de auditoría serán presentados a los Responsables del Sistema, al Delegado de Protección de Datos y a la Unidad de Seguridad TIC. Estos informes serán analizados por esta última, que presentará sus conclusiones a los Responsables del Sistema, y si fuese pertinente a los Responsables y Encargadas del Tratamiento, para que 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 normas de seguridad.

Artículo 19. Incidencia de la normativa de protección de datos personales.

1. Todos los tratamientos de datos personales que realice la Consejería se ajustarán a la normativa sobre protección de datos personales. En dicho ámbito, cada Responsable del Tratamiento de datos personales aplicará las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que los tratamientos de datos personales son conformes con dicha normativa, de acuerdo con el principio de responsabilidad proactiva. En caso de conflicto con otras normas de seguridad prevalecerá el criterio que presente un mayor nivel de exigencia respecto a la protección de datos personales.

2. Los Responsables y Encargados del Tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.

3. Cuando sea probable que un tipo de tratamiento 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. Para ello, recabará el asesoramiento del Delegado de Protección de Datos.

4. Cada Responsable del Tratamiento mantendrá un Registro de las Actividades de Tratamiento de datos personales efectuadas bajo su responsabilidad. Asimismo, cada Encargado del Tratamiento mantendrá un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de cada Responsable del Tratamiento. Estas labores se realizarán en coordinación con el Delegado de Protección de Datos y con la Unidad de Seguridad TIC, sin perjuicio de que la actualización, vigencia y calidad de la información del mismo sea responsabilidad de cada Responsable y Encargado del Tratamiento.

00164190

5. En caso de violación de la seguridad de los datos personales, el Responsable del Tratamiento lo pondrá en conocimiento inmediato del Delegado de Protección de Datos, que deberá asesorarle para proceder a notificar dicha violación a la autoridad de control competente, sin dilación y, de ser posible, antes de 72 horas desde que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Asimismo, 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 a la persona interesada sin dilación.

Artículo 20. Desarrollo de normas de seguridad de la información.

1. El conjunto de las normas sobre seguridad de la información es de obligado cumplimiento y se desarrollará en tres niveles con diferente ámbito de aplicación, detalle técnico y obligatoriedad de cumplimiento, pero de manera que cada elemento de desarrollo se fundamente en el nivel superior.

Todos estos niveles prestarán especial atención a las exigencias derivadas del Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, así como a la normativa aplicable en materia de protección de datos de carácter personal. Dichos niveles son los siguientes:

a) Primer nivel: Política de seguridad de la información y directrices y normas generales de seguridad de la información. Este tipo de normas deberán ser aprobadas por la persona titular de la Consejería.

b) Segundo nivel: Normas específicas de seguridad de la información, que desarrollan y detallan la política de seguridad de la información, centrándose en un área o aspecto determinado. Este tipo de normas deberán ser aprobadas por el Comité de Seguridad TIC de la Consejería.

c) Tercer nivel: Procedimientos, procesos, guías e instrucciones técnicas de seguridad de la información, que dan respuesta, incluyendo detalles de implementación y tecnológicos, a cómo se puede realizar una determinada tarea cumpliendo con lo expuesto en la política. Este tipo de normas deberán ser aprobadas por la persona titular del órgano directivo que tenga asignada las competencias relacionadas con la estrategia y aplicación de las tecnologías de la información y de las comunicaciones.

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

3. El Comité de Seguridad TIC establecerá los mecanismos necesarios para compartir la documentación relativa a normas de seguridad de la información con el propósito de normalizarlo, en la medida de lo posible, en todo el ámbito de aplicación de la política de seguridad de la información.

Artículo 21. Formación y concienciación en cultura de la seguridad de la información.

Anualmente se desarrollarán actividades de formación y concienciación sobre tratamiento de datos personales y seguridad de la información destinadas a las personas empleadas públicas en el ámbito de aplicación de esta norma. Entre tales actividades se incluirán las de difusión de la política de seguridad de la información y de su desarrollo normativo.

En la realización de esta actividad se tendrá en cuenta el plan de formación del Instituto Andaluz de Administración Pública para complementarlo con las acciones de la propia Consejería que sean necesarias.

00164190

Artículo 22. Cooperación 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 coordinación con al menos los siguientes agentes:

- Comité de Seguridad TIC de la Junta de Andalucía.
- Unidad de Seguridad TIC de la Junta de Andalucía.
- AndalucíaCERT (centro especializado y orientado a la prevención, detección y respuesta a incidentes y amenazas de seguridad).
- 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 Informativos Informáticos y Telemáticos de la Guardia Civil y Brigada de Investigación Tecnológica (BIT) del Cuerpo Nacional de Policía, para la investigación de acciones relacionadas con la delincuencia informática y los fraudes en el sector de las telecomunicaciones.

Adicionalmente, se podrán mantener contactos con otros organismos y entidades, incluyendo los entes instrumentales de la Consejería.

Artículo 23. Terceras partes.

1. Cuando la Consejería preste servicios a otros órganos o entes, o gestione información de otros órganos o entes, se les hará partícipes de esta política de seguridad de la información y de las normas de seguridad de la información que sean de aplicación, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad TIC, o en su defecto a los distintos responsables en materia de seguridad de la información enumeradas en la presente orden, y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

2. Cuando la Consejería utilice servicios de terceras partes o ceda información a terceras partes, se les hará partícipes de esta política de seguridad de la información y de las normas de seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dichas normas, pudiendo desarrollar sus propios procedimientos operativos para satisfacerlas. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que las personas empleadas de terceras partes estén adecuadamente concienciadas en materia de seguridad, al menos al mismo nivel que el establecido en la presente política. En su caso, a los efectos de articular estos preceptos, se preverán las cláusulas específicas que correspondan en relación con esta materia en los procesos de contratación de servicios de terceras partes así como en los acuerdos, convenios, encargos a medios propios personificados o cualquier otra figura jurídica que articule la relación con terceras partes.

3. Cuando algún aspecto de esta orden no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Será necesario que el contenido de este informe sea expresamente asumido por los Responsables de la Información y de los Servicios afectados. Si los Responsables de la Información y los Servicios no asumieran el contenido de dicho informe, podrían solicitar un nuevo informe, exponiendo los aspectos que no asumen. En caso de que mediante este método no se logre alcanzar una forma adecuada de tratar los riesgos, asumida por los Responsables de la Información y de los Servicios, deberá dejarse de prestar el servicio afectado por la tercera parte que no pueda satisfacer lo establecido en esta orden.

00164190

Artículo 24. Tratamiento de datos personales y observancia de la legislación vigente en la materia.

Para el tratamiento de datos personales en los sistemas de información se seguirá en todo momento lo establecido en el Reglamento general de protección de datos, así como lo establecido en la legislación nacional y autonómica vigente en cada momento en relación con esta materia.

Artículo 25. Prevención, detección, respuesta y recuperación de incidentes de seguridad.

1. Los órganos de la Consejería 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 (controles) determinadas por el Esquema Nacional de Seguridad, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles de seguridad deben estar claramente definidos y documentados. Para garantizar el cumplimiento efectivo de la presente política, los órganos de la Consejería deben realizar, en la medida de sus competencias, las siguientes actuaciones:

a) Autorizar los sistemas antes de entrar en operación.

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.

2. Dado que los servicios pueden degradarse rápidamente debido a incidentes, aquellos deben estar sometidos a monitorización de manera continua para detectar anomalías en sus niveles de prestación y así poder actuar con celeridad.

3. Los órganos de la Consejería deben establecer mecanismos para responder eficazmente a los incidentes de seguridad, así como designar un punto de contacto para las comunicaciones relativas a incidentes detectados en otros órganos o en otros organismos. Igualmente, deben establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con AndalucíaCERT.

4. Para garantizar la disponibilidad y recuperación de los servicios, los órganos de la Consejería deben desarrollar planes de continuidad para todos aquellos sistemas en los que así se haya requerido en el correspondiente Análisis de riesgos o sea exigible reglamentariamente.

5. Todas las actuaciones citadas en el presente artículo serán coordinadas por el Comité de Seguridad TIC.

Disposición adicional primera. Constitución del Comité de Seguridad TIC.

La primera reunión del Comité de Seguridad TIC tendrá por objeto la constitución del mismo y se celebrará en un plazo máximo de treinta días a partir de la entrada en vigor de la presente orden. En dicha reunión se procederá al nombramiento de la persona titular de la Unidad de Seguridad TIC. Asimismo, para aquella información, servicios y sistemas que se encuentren inventariados, se verificarán las designaciones de los Responsables de la Información, del Servicio y del Sistema.

Disposición adicional segunda. Actualización permanente y revisiones periódicas.

1. Esta orden deberá mantenerse actualizada para adecuarla a la evolución de los servicios TIC y, en general, a la evolución tecnológica y al desarrollo de la sociedad de la información, así como a los estándares internacionales de seguridad.

2. Las revisiones de la política de seguridad de la información se harán a propuesta del Comité de Seguridad TIC.

00164190

Disposición adicional tercera. Tribunal Administrativo de Recursos Contractuales.

Las menciones realizadas en los artículos 6.2, 8,1, 9.1 y 12.1 respecto a las personas titulares de los órganos directivos deberán entenderse también realizadas a la persona titular de la Presidencia del Tribunal Administrativo de Recursos Contractuales de la Junta de Andalucía.

Disposición adicional cuarta. Habilitación para ejecución y desarrollo.

Se habilita a la persona titular del órgano directivo que tenga asignada las competencias relacionadas con la estrategia y aplicación de las tecnologías de la información y de las comunicaciones para dictar cuantas actuaciones sean necesarias para la ejecución y desarrollo de lo establecido en 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.

Disposición final primera. Publicidad de la política de seguridad de la información.

A los efectos de su mejor difusión entre las personas empleadas de la organización y de otras partes interesadas, la presente orden se publicará, además de en el Boletín Oficial de la Junta de Andalucía, en los medios y soportes que se establezcan por el Comité de Seguridad TIC.

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, 21 de octubre de 2019

JUAN BRAVO BAENA
Consejero de Hacienda, Industria y Energía

00164190