1. Disposiciones generales

CONSEJERÍA DE EMPLEO, FORMACIÓN Y TRABAJO AUTÓNOMO

Orden de 31 de agosto de 2020, por la que se establece la política de seguridad de las tecnologías de la información y comunicaciones y de la protección de datos personales de la Consejería de Empleo, Formación y Trabajo Autónomo.

El artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece que el objeto del Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, regulado 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, es el establecimiento de la política de seguridad en la utilización de medios electrónicos y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada.

Su finalidad última es la creación de las condiciones necesarias 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, que permita a la ciudadanía y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

Para dar cumplimiento a los requisitos y finalidades del Esquema Nacional de Seguridad en su propio ámbito, la Junta de Andalucía aprobó 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, cuyo artículo 10 ordena que cada Consejería, en su ámbito de aplicación, disponga formalmente de su propio documento de política de seguridad de tecnologías de la información y las comunicaciones aprobado por su persona titular.

El citado Decreto creó un Comité de Seguridad de tecnologías de la información y las comunicaciones corporativo para toda la Junta de Andalucía dependiente de la Consejería competente en materia de dirección e impulso de la política de telecomunicaciones y seguridad de los sistemas de información, junto con un grupo de personas expertas en seguridad de tecnologías de la información y las comunicaciones de la Administración de la Junta de Andalucía.

Además, estableció que cada Consejería y ente instrumental de la Administración de la Junta de Andalucía debían constituir su propio Comité de Seguridad de tecnologías de la información y las comunicaciones mediante Orden de cada Consejería.

En la elaboración de esta Orden se ha tenido en cuenta la normativa actualmente aplicable en materia de datos personales, es decir, 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), así como la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

También se ha tenido en cuenta la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, conocida como «Directiva NIS».

La Orden consta de treinta y dos artículos, distribuidos en tres capítulos, dos disposiciones adicionales, una disposición derogatoria y una disposición final.

El capítulo I contiene las disposiciones generales sobre objeto y ámbito de aplicación.

El capítulo II se refiere a la política de seguridad de tecnologías de la información y las comunicaciones de la Consejería. En este capítulo se da cumplimiento en el ámbito de la

00177135

Consejería de Empleo, Formación y Trabajo Autónomo a dos obligaciones en materia de seguridad de tecnologías de la información y las comunicaciones impuestas tanto por el Esquema Nacional de Seguridad como por la normativa reguladora de dicha política de seguridad en la Administración de la Junta de Andalucía.

Por un lado, establece la estructura de organización y gestión de la seguridad de tecnologías de la información y las comunicaciones de la Consejería y por otro, aprueba el Documento de Política de Seguridad en esta materia dentro del ámbito de sus competencias.

El capítulo III está dedicado a aspectos organizativos para recoger la incidencia de la normativa de protección de datos, y especialmente del Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y la Ley Orgánica 3/2018, de 5 de diciembre, que afectan directamente a la seguridad TIC.

En la elaboración y tramitación de la presente orden, se ha actuado conforme a los principios de buena regulación a los que se refiere el artículo 129.1 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y se ha tenido en consideración el principio de transversalidad de género según se estable en el artículo 5 de la Ley 12/2007, de 26 de noviembre, para la promoción de la igualdad de género en Andalucía.

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

En su virtud, conforme a lo establecido en los artículos 44.2 y 46.4 de la Ley 6/2006, de 24 de octubre, del Gobierno de la Comunidad Autónoma de Andalucía, el artículo 26.2.a) de la Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía, así como en el Decreto 100/2019, de 12 de febrero, por el que se regula la estructura orgánica de la Consejería de Empleo, Formación y Trabajo Autónomo,

D I S P O N G O

CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 1. Objeto.

1. La presente Orden tiene por objeto establecer la política de seguridad de las tecnologías de la información y comunicaciones, en adelante seguridad TIC, en el ámbito de la Consejería de Empleo, Formación y Trabajo Autónomo, en adelante la Consejería, de acuerdo con la normativa reguladora de la política de seguridad TIC de la Administración de la Junta de Andalucía, en el marco de la normativa reguladora del Esquema Nacional

00177135

de Seguridad en el ámbito de la Administración Electrónica, en adelante ENS, y de la normativa en materia de protección de datos personales.

2. La presente Orden constituye el Documento de Política de Seguridad TIC de la Consejería.

Artículo 2. Ámbito de aplicación.

1. La política de seguridad TIC se aplicará a todos los sistemas de información que son responsabilidad de la Consejería de Empleo, Formación y Trabajo Autónomo, para el ejercicio de las competencias que tiene atribuidas, siempre que sean utilizados en el ámbito de la Administración de la Junta de Andalucía, por alguno de los órganos o unidades administrativas centrales o periféricos que dependan funcionalmente de la Consejería. Asimismo, deberá ser observada por todo el personal de la Junta de Andalucía destinado en dichos órganos y unidades administrativas, así como por aquellas personas que tengan acceso a sus sistemas de información.

2. La política de seguridad TIC definida en esta orden también será de obligado cumplimiento para sus entidades vinculadas o dependientes de la Consejería, de conformidad con el artículo 10.3 del Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía.

Artículo 3. Marco normativo.

1. Se asume como marco regulador general el que en cada momento se defina, en virtud de la disposición adicional primera del Decreto 1/2011, de 11 de 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 este organismo en virtud de su naturaleza legal y sus competencias.

2. La Consejería podrá ampliar y desarrollar el marco normativo en los términos previstos en la disposición adicional segunda.

CAPÍTULO II

POLÍTICA DE SEGURIDAD TIC

Artículo 4. Objetivos.

Son objetivos de la política de seguridad TIC, de acuerdo con el artículo 4 del Decreto 1/2011, de 11 de enero:

a) Garantizar la seguridad TIC y proteger los activos o recursos de información.

b) Crear la estructura de la organización de la seguridad TIC de la Consejería.

c) Marcar las directrices, los objetivos y los principios básicos de seguridad TIC de la Consejería.

d) Orientar la organización para la prestación de servicios basados en la gestión de riesgos.

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

Artículo 5. Principios básicos.

Los principios básicos que regirán la política de seguridad TIC de la Consejería serán, conforme a la normativa reguladora de la política de seguridad TIC en la Administración de la Junta de Andalucía y en el ENS, los siguientes:

a) Principio de prevención: Se evitará, o al menos prevendrá en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello, se deben implementar las medidas mínimas de seguridad determinadas

00177135

por las normas y leyes que le sean de aplicación, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, estarán claramente definidos y documentados.

b) Principio de detección: Dado que los servicios se pueden degradar rápidamente debido a incidentes que, en función de su gravedad, pueden producir desde una simple desaceleración hasta la detención de los mismos, se debe monitorizar la operación de los servicios de manera continua para detectar anomalías en los niveles de prestación requeridos, actuando en consecuencia. La monitorización es especialmente relevante para establecer líneas de defensa. Para ello, se implantarán mecanismos de detección, análisis y reporte que lleguen a las personas responsables regularmente, a efectos de detectar cuándo se produce una desviación significativa de los parámetros de servicio marcados.

c) Principio de reacción: Deberá minimizarse el tiempo requerido de recuperación, de forma que el impacto de los incidentes de seguridad sea el menor posible, para lo cual se establecerán mecanismos para responder eficazmente a los incidentes de seguridad, designando un punto de contacto para centralizar y gestionar el intercambio de información asociada a los incidentes de seguridad, así como estableciendo protocolos para el intercambio de información relacionada con dichos incidentes y las notificaciones que puedan ser necesarias en caso de que haya datos personales afectados.

d) Principio de recuperación: Se deberá garantizar en la medida de lo posible la disponibilidad de los servicios ofrecidos a la ciudadanía, en función de la criticidad de los mismos.

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

f) Integridad y confidencialidad de los datos personales: Los datos personales serán tratados de tal manera que se garantice una seguridad adecuada de los mismos, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.

Artículo 6. Organización y gestión de la seguridad TIC.

1. La estructura organizativa de la gestión de la seguridad TIC de la Consejería, en relación con el ENS, está compuesta por las siguientes figuras:

a) Comité de Seguridad TIC.

b) Unidad de Seguridad TIC, la persona responsable de esta Unidad de Seguridad tendrá la condición de Responsable de Seguridad TIC.

c) Responsables de la Información.

d) Responsables de los Sistemas.

e) Responsables de los Servicios.

2. Además, en el ámbito de la Consejería, las siguientes figuras ostentan atribuciones directamente relacionadas con la seguridad TIC que son las que les asigna la normativa sobre protección de datos personales:

a) Responsables de los tratamientos de datos personales.

b) Encargados o encargadas de los tratamientos de datos personales.

c) Delegado o Delegada de Protección de Datos.

3. El Servicio Andaluz de Empleo, de acuerdo con la disposición adicional segunda del Decreto 1/2011, de 11 de enero, contará con su propio Comité y Unidad de Seguridad TIC, rigiéndose por la Resolución de 25 de junio de 2019, del Servicio Andaluz de Empleo, por la que se aprueba la Política de Seguridad TIC en el ámbito de la Agencia.

00177135

En este sentido, dentro de su ámbito competencial, en materia de seguridad TIC, tendrá la siguiente estructura:

a) Comité de Seguridad TIC.

b) Unidad de Seguridad TIC, la persona responsable de esta Unidad de Seguridad tendrá la condición de Responsable de Seguridad TIC.

c) Responsables de la Información.

d) Responsables de los Sistemas.

e) Responsables de los Servicios.

Igualmente, el ámbito de la Agencia, las siguientes figuras ostentan atribuciones directamente relacionadas con la seguridad TIC que son las que les asigna la normativa sobre protección de datos de personales:

a) Responsables de los tratamientos de datos personales.

b) Encargados o encargadas de los tratamientos de datos personales.

c) Delegado o Delegada de Protección de Datos.

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

Artículo 7. Creación del Comité de Seguridad TIC.

1. Se crea el Comité de Seguridad TIC de la Consejería, como órgano con carácter no colegiado.

2. El Comité de Seguridad TIC actuará como órgano de dirección y seguimiento en materia de seguridad de los activos TIC de titularidad de la Consejería o cuya gestión tenga encomendada.

3. El Comité de Seguridad TIC de la Consejería articulará los mecanismos de colaboración y coordinación necesarios con los de sus entidades vinculadas o dependientes, tal como indica el artículo 10.5 del Decreto 1/2011, de 11 de enero.

Artículo 8. Funciones del Comité de Seguridad TIC.

1. Al Comité le corresponde aplicar, en el ámbito de la Consejería, las previsiones contenidas en la normativa reguladora del ENS, y en la normativa reguladora de la política de seguridad TIC en la Administración de la Junta de Andalucía y determinar la política de seguridad que se ha de emplear en la utilización de los medios electrónicos que permita la adecuada protección de la información.

2. En particular, le corresponde:

a) Aprobar el desarrollo de la política de seguridad TIC de segundo nivel, según lo previsto en el artículo 19.

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

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

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

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

00177135

f) Velar para que todos los ámbitos de responsabilidad y actuación en relación a la seguridad TIC y su tratamiento queden perfectamente definidos, aprobando los nombramientos de su competencia necesarios para ello. Asimismo, asegurar que todos y cada uno de los miembros de la estructura de seguridad definida conozcan sus funciones y responsabilidades.

g) Nombrar la Unidad de Seguridad TIC de la Consejería designando su persona responsable que ostentará la condición de Responsable de Seguridad TIC de la Consejería.

h) Promover y fomentar la divulgación y formación en cultura de la seguridad TIC y la protección de datos personales, así como la mejora continua de la seguridad en la organización, aprobando los planes de mejora de seguridad TIC propuestos por la Unidad de Seguridad TIC, y velando por la asignación y cumplimiento de las responsabilidades oportunas. Para llevar las labores de divulgación y formación, podrá contarse con la figura del Delegado o de la Delegada de Protección de Datos.

i) Velar por que la seguridad TIC 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, garantizando el acceso a los datos personales solo a quienes deban tratar los mismos.

j) Asegurar que el desarrollo normativo que tenga incidencia en el desarrollo o explotación de sistemas de información se adecua a lo establecido en la política de seguridad TIC.

k) Resolver los conflictos que puedan aparecer entre las diferentes personas responsables o entre diferentes áreas de la organización en materia de seguridad TIC, siempre que no exista un superior jerárquico común entre ellos.

l) Coordinar las medidas técnicas y organizativas establecidas en la normativa de protección de datos personales, de acuerdo con los correspondientes análisis de riesgos y, en su caso, las evaluaciones de impacto en la protección de datos, contando con el asesoramiento del Delegado o Delegada de Protección de Datos.

m) Coordinar el Documento de Seguridad en los términos exigidos por la normativa de protección de datos personales.

Artículo 9. Composición del Comité de Seguridad TIC.

1. El Comité de Seguridad TIC estará compuesto por los siguientes miembros:

a) Presidencia: La persona titular de la Viceconsejería. Tendrá voto de calidad en la toma de decisiones del Comité en caso de empate.

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

c) Vocalías: Las personas titulares de todos los órganos directivos centrales, las personas titulares de todos los órganos directivos de las delegaciones territoriales y la persona titular de la Coordinación General de la Secretaría General Técnica.

d) Secretaría: La persona titular de la Jefatura del Servicio de Informática, con voz y voto.

2. 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 designarán una persona que les sustituya en estas circunstancias entre personal funcionario que ocupen puestos de trabajo de nivel 28 o superior. En el caso de la Secretaría, será sustituida por una persona funcionaria adscrita al Servicio de Informática, que designe la presidencia del Comité de Seguridad TIC.

3. En la composición del Comité ha de garantizarse la representación equilibrada de mujeres y hombres, 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. En caso de necesidad de suplencia de alguno de sus miembros corresponderá a la Secretaría velar porque se siga cumpliendo la representación equilibrada en la composición del Comité.

00177135

4. La persona responsable de la Unidad de Seguridad TIC y la persona que ostente la condición de Delegado o Delegada de Protección de Datos asistirán en calidad de asesoras a las reuniones del Comité de Seguridad TIC, salvo que puntualmente se disponga lo contrario de forma expresa y motivada por parte de la presidencia. El Comité de Seguridad TIC podrá convocar a sus reuniones a las personas que en cada caso autorice la presidencia, por propia iniciativa o a propuesta de alguno de sus miembros. Asimismo podrá recabar de personal técnico especializado, propio o externo, la información pertinente para la toma de decisiones.

Artículo 10. Funcionamiento del Comité de Seguridad TIC.

1. El Comité de Seguridad TIC se reunirá con carácter ordinario una vez al año y con carácter extraordinario por acuerdo de la presidencia, a iniciativa propia o previa solicitud razonada de uno de sus miembros.

2. El Comité se podrá constituir, convocar, celebrar sus sesiones, adoptar acuerdos y remitir actas, tanto de forma presencial como utilizando redes de comunicación a distancia, con las medidas adecuadas que garanticen la identidad de las personas comunicantes y la autenticidad de la información entre ellas transmitida, de conformidad con lo establecido en el artículo 91.3 de la Ley 9/2007, de 22 de octubre, y los artículos 17 y 18 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. A los efectos de convocatorias, requisitos para celebración de sesiones, mayorías necesarias para adopción de acuerdos, votos dirimentes en caso de empate o funciones de sus integrantes, se estará a lo previsto en dichos artículos 17 y 18 de la Ley 40/2015, de 1 de octubre.

Artículo 11. Régimen jurídico del Comité de Seguridad TIC.

El Comité de Seguridad TIC se regirá por esta Orden, por la normativa reguladora de la política de seguridad TIC en la Administración de la Junta de Andalucía, la reguladora del ENS, la normativa de protección de datos personales, así como por el resto de normativa aplicable.

Artículo 12. Unidad de Seguridad TIC.

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

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

a) Dar soporte, asesorar e informar al Comité de Seguridad TIC de la Consejería, así como ejecutar las decisiones y acuerdos adoptados por éste y gestionar la documentación derivada de los distintos niveles de seguridad.

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

c) Definir, implantar y mantener los controles de carácter organizativo para la protección de los datos, aplicaciones y sistemas, así como realizar y mantener los análisis de riesgos de la Consejería, en colaboración con el Delegado o Delegada de Protección de Datos.

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

00177135

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

f) Definir y ejecutar los programas formativos y de concienciación relacionados con buenas prácticas de seguridad TIC y protección de datos personales en el ámbito de la Consejería. Para llevar las labores mencionadas, podrá contarse con la figura del Delegado o de la Delegada de Protección de Datos

g) Coordinar, dirigir y seguir la actividad en materia de seguridad TIC de las entidades vinculadas o dependientes de la Consejería, en el momento en que se apruebe la política de seguridad TIC de dichas entidades.

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

i) Y cuantas otras le sean encomendadas por la Viceconsejería, en cuanto presidencia del Comité de Seguridad TIC.

3. Asimismo, esta Unidad de Seguridad TIC velará por la adopción de las medidas en materia de gestión de incidentes de seguridad TIC, conforme a las normas que se establezcan sobre la gestión de dichos incidentes, en coordinación con el Delegado o la Delegada de Protección de Datos.

Artículo 13. Responsable de Seguridad TIC.

La persona responsable de la Unidad de Seguridad TIC de la Consejería tendrá la condición de Responsable de Seguridad TIC, en los términos establecidos en la normativa reguladora del ENS.

Artículo 14. Responsables de la Información.

1. Las personas Responsables de la Información serán las personas titulares de los órganos directivos que decidan sobre la finalidad, contenido y uso de la información.

2. Las funciones, dentro de su ámbito de actuación, son las siguientes:

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

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, incluyendo el resultado de los análisis de riesgos o las evaluaciones de impacto de protección de datos personales. Para ello contará con la ayuda de las personas Responsables de los Servicios y Responsables de los Sistemas.

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

3. 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 15. Responsables de los Servicios.

1. Las personas Responsables de los Servicios serán las personas titulares de los órganos directivos que decidan sobre las características de los servicios a prestar.

2. Las funciones, dentro de su ámbito de actuación, son las siguientes:

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

00177135

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 las personas Responsables de la Información y Responsables de los Sistemas.

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

3. El nombramiento o renovación de las personas responsables de los servicios 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 16. Responsables de los Sistemas.

1. Responsables de los Sistemas serán aquellas personas adscritas al Servicio con competencias en materia de Informática que sean designadas al efecto por la persona titular de la jefatura de dicho Servicio y figurarán en la documentación de seguridad de los sistemas de información. Para cada sistema de información deberá existir una persona Responsable de Sistema, siendo posible que una misma persona sea responsable de varios sistemas o de todos ellos.

2. Sus responsabilidades serán:

a) Supervisar el desarrollo, operación y mantenimiento de los sistemas de información durante todo su ciclo de vida, así como las especificaciones de los mismos, la instalación y verificación de su correcto funcionamiento.

b) Ser la primera persona responsable de la seguridad de los sistemas de información que dirija, velando porque la seguridad TIC esté presente en todas y cada una de las partes de sus ciclos de vida. Especialmente, deberá velar para que el desarrollo de los sistemas siga las directrices de seguridad establecidas de manera horizontal por la Junta de Andalucía de acuerdo con los criterios y requisitos técnicos de seguridad aplicables definidos por la Unidad de Seguridad TIC de la Consejería.

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) Asesorar en la definición de la topología y sistema de gestión de los sistemas de información estableciendo los criterios de uso y los servicios disponibles en el mismo.

e) Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema.

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

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

h) Suspender el manejo de una cierta información o la prestación de un cierto 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 las personas Responsables de la Información afectada, del Servicio afectado y con la Unidad de Seguridad TIC, antes de ser ejecutada y trasladada al Delegado o Delegada de Protección de Datos si hubiera datos personales afectados.

Artículo 17. Resolución de conflictos.

1. Los conflictos entre las diferentes personas, unidades u órganos responsables que componen la estructura organizativa de la política de seguridad TIC serán resueltos por el superior jerárquico común. En su defecto, 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 la normativa de protección de datos personales prevalecerá la decisión que presente un mayor nivel de exigencia respecto a la protección de los datos personales. En caso de

00177135

conflicto en la determinación de dicho nivel de exigencia, prevalecerán las decisiones del Comité de Seguridad TIC adoptadas en sesión plenaria.

Artículo 18. Obligaciones del personal.

1. Todo el personal que preste servicios en la Consejería tiene la obligación de conocer y cumplir la política de seguridad TIC y la normativa de seguridad derivada, siendo responsabilidad del Comité de Seguridad TIC disponer los medios necesarios para que la información llegue a las personas afectadas.

2. Todo el personal que se incorpore a la Consejería o vaya a tener acceso a alguno de sus sistemas de información o la información gestionada por ellos deberá ser informado de la política de seguridad TIC. Asimismo, deberá cumplir además con las instrucciones y normas que regulen el comportamiento del personal empleado público en el uso de los sistemas informáticos y redes de comunicaciones de la Administración de la Junta de Andalucía

3. Procederá el ejercicio de las acciones pertinentes para la exigencia de las responsabilidades legales que correspondan por el incumplimiento manifiesto de la política de seguridad TIC o de la normativa de seguridad derivada.

4. Cualquier persona que actúe bajo la autoridad de la persona Responsable o Encargada de un Tratamiento de datos personales en el ámbito de aplicación de esta Orden y tenga acceso a datos personales solo tratará dichos datos siguiendo instrucciones de la persona responsable, salvo que se lo impida el ordenamiento jurídico comunitario, nacional o autonómico. Y en ningún caso podrá tratar datos personales para los que no esté autorizado en el ejercicio de sus competencias, debiendo informar a la persona Responsable del Tratamiento cuando tenga acceso a datos personales que queden fuera de sus competencias para que se adopten las medidas necesarias.

5. Anualmente se desarrollarán actividades de formación y concienciación en seguridad TIC y protección de datos personales, destinadas al personal adscrito a los órganos y unidades administrativas comprendidas en el ámbito de aplicación de la presente Orden. Entre tales actividades se incluirán las de difusión de esta política de seguridad TIC y de su desarrollo normativo.

Artículo 19. Desarrollo.

1. Las medidas sobre la seguridad TIC, de obligado cumplimiento, se desarrollarán en cuatro 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. Dichas medidas conformarán el Plan Director de Seguridad de los Sistemas de Información de la Consejería. Además, se observará lo establecido en la disposición adicional primera del Decreto 1/2011, de 11 de enero.

2. Todos estos niveles prestarán especial atención a las exigencias derivadas del ENS, así como a la normativa aplicable en materia de protección de datos personales.

3. Los niveles de desarrollo son los siguientes:

a) Primer nivel: Política de seguridad TIC, constituido por la presente Orden. Es de obligado cumplimiento en toda la Consejería.

b) Segundo nivel: Normas de seguridad. Son de obligado cumplimiento en toda la Consejería y deben ser aprobadas por el Comité de Seguridad TIC. Describen de forma general los principios y normas de seguridad que serán concretados en los niveles posteriores.

c) Tercer nivel: Procedimientos. Describen las acciones a realizar, de una manera más específica, en un proceso relacionado con la seguridad. Son dependientes de las normas de seguridad. Los aprueba la persona titular de la Secretaría General Técnica.

d) Cuarto nivel: Documentación técnica. En este último nivel se puede incluir todo tipo de documentación técnica o especializada que se considere necesario para completar y facilitar el desarrollo de las medidas de seguridad. La aprueba la persona titular de la

00177135

jefatura del Servicio de Informática o quien sea Responsable del Sistema en el caso del artículo 16.

4. El Comité de Seguridad TIC establecerá los mecanismos necesarios para compartir la documentación derivada del desarrollo con el propósito de regularizarlo, en la medida de lo posible, en todo el ámbito de aplicación de la política de seguridad TIC.

Nivel	Documento	Aprueba
Primero	Política de seguridad	Persona titular de la Consejería
Segundo	Normas de seguridad	Comité de Seguridad TIC
Tercero	Procedimientos	Persona titular de la Secretaría General Técnica
Cuarto	Documentación técnica	Persona titular de la jefatura del Servicio de Informática o quien sea Responsable del Sistema en el caso del artículo 16.

5. La Unidad de Seguridad TIC se encarga de la gestión de los documentos indicados, debiendo asegurar que esta sea completa y proporcione información suficiente para definir las necesidades de protección de la información y los activos asociados a la misma en el ámbito de la Consejería. La disponibilidad y difusión se exceptuará en aquellas cuestiones que puedan suponer un riesgo a la seguridad de los sistemas de información o los datos, especialmente en el caso de datos personales.

Artículo 20. Gestión de riesgos.

1. La gestión de riesgos deberá realizarse de manera continua sobre el sistema de información, conforme a los principios de gestión de la seguridad basada en los riesgos y con reevaluación periódica de los mismos.

2. Las personas encargadas de la categorización de los sistemas serán las Responsables de la Información y de los Servicios, siendo la Unidad de Seguridad TIC la encargada de supervisar los análisis de riesgos y proponer las medidas de seguridad a aplicar.

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

4. Tanto Responsables de la Información como de los Servicios asumirán la responsabilidad de aceptar los riesgos residuales calculados en el análisis sobre la información y los servicios, respectivamente. También serán responsables de realizar su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea en personal de su órgano directivo o ámbito de actuación.

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, que deberán ser proporcionales a los riesgos y estar justificadas, deberá revisarse al menos con periodicidad anual por parte de la Unidad de Seguridad TIC, que elevará un informe al Comité de Seguridad TIC. En dicha revisión, podrá participar el Delegado o la Delegada de Protección de Datos.

Artículo 21. Clasificación y control de activos.

1. Los recursos informáticos y la información de la Consejería se encontrarán inventariados, con una persona responsable asociada y, en caso de ser necesario, una persona responsable de la custodia de los mismos. Los inventarios se mantendrán actualizados para asegurar su validez.

2. Los activos de información estarán clasificados de acuerdo a su sensibilidad y criticidad para el desarrollo de la actividad de la Consejería, en función de la cual se establecerán las medidas de seguridad exigidas para su protección.

00177135

Artículo 22. Auditorías de la seguridad.

1. Los sistemas de información serán objeto de una auditoría regular ordinaria, al menos cada dos años, que verifique el cumplimiento de los requerimientos del ENS. Estas auditorías ordinarias así como las extraordinarias se harán de acuerdo con lo establecido en el art. 34 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, y la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información aprobada en cada momento, así como la normativa vigente.

2. Los informes de auditoría serán presentados a la persona Responsable del Sistema competente, al Delegado o Delegada de Protección de Datos, si afectara a éstos, y a la persona responsable de la Unidad de Seguridad TIC. Estos informes serán analizados por esta última persona que presentará sus conclusiones a la persona Responsable del Sistema para que adopte las medidas correctoras adecuadas; y al Delegado o Delegada de Protección de Datos para su conocimiento. Los resultados obtenidos determinarán las líneas de actuación a seguir y las posibles modificaciones a realizar sobre los controles y la normativa de seguridad.

3. Con el fin de optimizar la utilización de los recursos públicos y garantizar una mejor coordinación entre seguridad TIC y seguridad de protección de datos, siempre que sea posible, las auditorías de seguridad de sistemas de información y las auditorías de protección de datos o medidas análogas de verificación, evaluación y valoración de seguridad de los tratamientos se realizarán de manera conjunta.

Artículo 23. Terceras partes.

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

2. Cuando algún órgano utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta política de seguridad TIC y de la normativa de seguridad TIC que ataña a dichos servicios o información. Dicha tercera parte, quedará sujeta, a través de cláusulas contractuales en el marco de una contratación, o mediante cualquier otro tipo de vinculación o acuerdo entre las partes, a las obligaciones generales establecidas en dicha normativa, pudiendo disponer la tercera parte de sus propios procedimientos operativos para satisfacerla. Se establecerán mecanismos de comunicación y resolución de incidencias. Se velará por que el personal de terceros esté adecuadamente concienciado en materia de seguridad, al menos, al mismo nivel que el establecido en esta política de seguridad TIC.

3. Cuando algún aspecto de esta política de seguridad TIC no pueda ser satisfecho por una tercera parte según se requiere en el párrafo anterior, se requerirá un informe de la Unidad de Seguridad TIC que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por cada Responsable de Información y/o Servicio afectado antes de proseguir en la relación con la tercera parte. Cuando ello ocurra con datos personales se entenderá que la tercera parte no es la adecuada para el tratamiento de datos propuesto y no podrá considerarse por tanto su participación.

Artículo 24. Cooperación con otros órganos y otras administraciones en materia de seguridad.

1. 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) Comité de Seguridad TIC de la Junta de Andalucía.

00177135

b) Unidad de Seguridad TIC Corporativa.

c) AndaluciaCERT, como 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.

d) Consejo de Transparencia y Protección de Datos de Andalucía.

e) 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.

f) Instituto Nacional de Ciberseguridad (INCIBE)

g) Grupo de Delitos Telemáticos de la Guardia Civil y Brigada de Investigación Tecnológica del Cuerpo Nacional de Policía, para la investigación de acciones relacionadas con la delincuencia informática y los fraudes en el sector de las telecomunicaciones.

2. En los casos de comunicación con agentes externos a la Junta de Andalucía, esta se llevará a cabo de manera coordinada con la Unidad de Seguridad TIC Corporativa.

CAPÍTULO III

PROTECCIÓN DE DATOS PERSONALES

Artículo 25. Incidencia de la normativa de protección de datos personales.

1. Todos los sistemas de información de la Consejería y de sus entidades dependientes y vinculadas se ajustarán a lo exigido por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, por el que se aprueba el Reglamento General de Protección de Datos, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y el resto de la normativa general o sectorial de protección de datos personales que sea de aplicación. Todos los tratamientos de datos personales, automatizados o no automatizados, se sujetarán a la citada norma cuando se encuentren dentro de su ámbito de aplicación.

2. 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 personales, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, y de conformidad con el artículo 32 del Reglamento General de Protección de Datos, la persona Responsable y la Encargada 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, de acuerdo con la disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre, de modo que estas deberán tomarse de las previstas en el ENS y que en su caso incluya, entre otras:

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.

Artículo 26. Evaluación del impacto de las operaciones de tratamiento.

De conformidad con el artículo 35 del Reglamento General de Protección de Datos, 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 tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos

00177135

riesgos similares. La autoridad de control en materia de protección de datos determinará según los apartados 4 y 5 del artículo 35 del Reglamento General de Protección de Datos, cuando será obligatorio y cuando no la realización de la evaluación de impacto. Para realizar la evaluación, se podrá recabar el asesoramiento del Delegado o Delegada de Protección de Datos.

Artículo 27. Registro de actividades de tratamiento.

1. La persona Responsable del Tratamiento llevará un registro de las actividades de tratamiento de datos personales efectuadas bajo su responsabilidad, de acuerdo con lo establecido en el artículo 30 del Reglamento General de Protección de Datos y el resto de normativa de datos personales aplicable. Cada Encargado o Encargada del Tratamiento llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un Responsable, de acuerdo con el mismo precepto.

2. En virtud de lo establecido en el artículo 31.1 de la Ley Orgánica 3/2018, de 5 de diciembre, cuando la persona Responsable o Encargada del Tratamiento hubiera designado un Delegado o Delegada de Protección de Datos, deberá comunicarle cualquier adición, modificación o exclusión en el contenido del registro.

Artículo 28. 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, de ser posible, a más tardar 72 horas después de 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. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de 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, la persona Responsable del Tratamiento la comunicará a las personas interesadas sin dilación indebida. Dicha notificación y comunicación se atendrán a lo establecido en los artículos 33 y 34 del Reglamento General de Protección de Datos y el resto de normativa de datos personales aplicable.

2. La notificación a la autoridad de control a la que se refiere el apartado anterior podrá realizarse a través de AndalucíaCERT y del Centro Criptológico Nacional, siempre que se cumplan los requisitos del Reglamento General de Protección de Datos, en los casos en los que así lo disponga la política de seguridad TIC de la Junta de Andalucía. En todo caso se deberá informar de ello al Delegado o Delegada de Protección de Datos, preferiblemente de manera paralela a la autoridad de control.

Artículo 29. Responsables de los Tratamientos de datos personales.

1. Las personas Responsables de los Tratamientos de datos personales 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 Reglamento General de Protección de Datos.

2. En el ámbito de la política de seguridad TIC de esta Consejería, las personas Responsables de la Información, es decir, las personas titulares de los órganos directivos, tendrán la condición de Responsables del Tratamiento respecto a los tratamientos sobre los que determinen sus fines y medios, salvo que las normas aplicables sobre asignación de atribuciones en materia de protección de datos personales dispongan otra cosa.

3. Cada Responsable del Tratamiento de datos personales aplicará las medidas técnicas y organizativas apropiadas a fin de garantizar y ser capaz de demostrar que los tratamientos de datos personales son conformes con dicha normativa, de acuerdo con el principio de responsabilidad proactiva, de conformidad con el artículo 24 del Reglamento General de Protección de Datos. En caso de conflicto con la normativa de seguridad

00177135

prevalecerá el criterio que presente un mayor nivel de exigencia respecto a la protección de los datos personales.

4. El nombramiento o renovación de las personas responsables 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 30. Encargados de los Tratamientos de datos personales.

1. Si las personas Responsables de los Tratamientos designaran a un Encargado o Encargada del Tratamiento lo harán únicamente cuando éste ofrezca garantías suficientes para aplicar las medidas técnicas y organizativas apropiadas para que el tratamiento sea conforme al artículo 38. 1 del Reglamento General de Protección de Datos 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 Reglamento General de Protección de Datos y demás normativa de aplicación.

3. Conforme a lo establecido en el artículo 29 del Reglamento General de Protección de Datos, la persona Encargada del Tratamiento y cualquier persona que actúe bajo la autoridad de la persona Responsable o Encargada, y tenga acceso a datos personales solo podrá tratar dichos datos siguiendo instrucciones de la persona responsable, a no ser que estén obligados en virtud de la normativa vigente.

Artículo 31. Delegado o Delegada de Protección de Datos.

1. Existirá una persona que ostente la condición de Delegado o Delegada de Protección de Datos a efectos de lo establecido en los artículos 37 y 38 del Reglamento General de Protección de Datos.

2. La persona que ostente la condición de Delegado o Delegada de Protección de Datos será designada por la persona titular de la Viceconsejería 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. La Resolución por la que se la designe determinará los órganos o unidades administrativas centrales o periféricos que dependan funcionalmente de la Consejería o estén adscritos a la Consejería respecto a los que ejercerá sus funciones.

3. El Delegado o Delegada de Protección de Datos de la Consejería colaborará y se coordinará con las entidades vinculadas o dependientes de la misma en todas las cuestiones relativas a su ámbito de competencia, estableciendo mecanismos de colaboración con las personas responsables de protección de datos de dichas entidades.

Artículo 32. Funciones del Delegado o Delegada de Protección de Datos.

Son funciones del Delegado o Delegada de Protección de Datos, además de lo establecido en el artículo 39 del Reglamento General de Protección de Datos y el artículo 37 de la Ley Orgánica 3/2018, de 5 de diciembre, las siguientes:

a) Informar previa consulta o a iniciativa propia sobre la contratación, análisis, diseño, operación y mantenimiento de los tratamientos realizados sobre datos personales. También sobre todo proyecto normativo que suponga un tratamiento de datos personales, aplicando a la organización el principio de responsabilidad proactiva.

b) Asesorar y velar, desde la posición que le atribuye el artículo 38 del Reglamento General de Protección de Datos, por el correcto ejercicio de los derechos de las personas interesadas recogidos en el Capítulo III del Reglamento General de Protección de Datos, en especial cuando se requiera la respuesta coordinada de diferentes responsables del tratamiento, así como al Comité de Seguridad TIC en lo que a sistemas de información se refiere.

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

00177135

d) Supervisar que los encargos del tratamiento sobre categorías de datos que requieran una evaluación del impacto sobre la privacidad, por aplicación del artículo 35 del Reglamento General de Protección de Datos, recojan en su articulado las medidas de seguridad atribuibles a la persona Encargada del Tratamiento y determinadas por las personas Responsables del Tratamiento para afrontar los riesgos evaluados.

e) Asesorar sobre la confección de los modelos de formularios que supongan recogida de datos personales.

f) Supervisar la gestión del Registro de Actividades de Tratamiento de las personas Responsables del Tratamiento de la Consejería, debiendo éstos facilitarle la información necesaria para ello.

g) Asesorar a la persona Responsable del Tratamiento sobre la oportunidad y modo de comunicar a las personas interesadas y afectadas por violaciones de la seguridad de sus datos personales que entrañen un alto riesgo para los derechos y libertades de las personas físicas, conforme a lo establecido en el artículo 34 del Reglamento General de Protección de Datos.

h) Poner en conocimiento del Comité de Seguridad TIC las cuestiones relacionadas con la protección de datos personales que considere oportunas y participar, si lo estimase conveniente, 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.

i) Participar en tareas de formación y divulgación relativas al ámbito de la protección de datos personales.

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 un mes a partir de la entrada en vigor de la presente Orden. En dicha reunión constitutiva se procederá al nombramiento de la Unidad de Seguridad TIC, así como la designación de su persona responsable y la determinación de las distintas personas Responsables de la Información y de los Servicios.

Disposición adicional segunda. Desarrollo y ejecución.

Se faculta a la persona titular de la Secretaría General Técnica de la Consejería para dictar cuantas instrucciones sean necesarias y adoptar cuantas medidas técnicas sean oportunas para el desarrollo, difusión y ejecución 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 esta Orden.

Disposición final única. 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, 31 de agosto de 2020

ROCÍO BLANCO EGUREN
Consejera de Empleo, Formación
y Trabajo Autónomo

00177135