1. Disposiciones generales

CONSEJERÍA DE LA PRESIDENCIA, ADMINISTRACIÓN LOCAL Y MEMORIA DEMOCRÁTICA

Orden de 30 de agosto de 2018, por la que se establece la política de la seguridad de las tecnologías de la información y telecomunicaciones así como el marco organizativo y tecnológico en el ámbito de la Consejería.

00141662

El Esquema Nacional de Seguridad en el ámbito de la administración electrónica (ENS) cuyo objeto es el establecimiento de los principios y requisitos de una política de seguridad en la utilización de medios electrónicos que permita la adecuada protección de la información, actualmente incluido en el artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, se regula por el Real Decreto 3/2010, de 8 de enero, que regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, aún en vigor.

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 ENS 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 TIC aprobado por su persona titular.

El citado Decreto creó un Comité de Seguridad de las Tecnologías de la Información y Comunicaciones (TIC) 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 TIC 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 TIC mediante Orden de cada Consejería.

Por otro lado, para la gestión ordinaria de la seguridad disponía la existencia de un Responsable de Seguridad corporativo y uno en cada Consejería o ente instrumental a designar por el respectivo Comité de Seguridad TIC. Esta figura asumiría las funciones de Responsable de Seguridad descritos en la normativa reguladora del Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Recientemente, el Decreto 70/2017, de 6 de junio, ha modificado el Decreto 1/2011, de 11 de enero. Dicha modificación, según su exposición de motivos, responde a la necesidad de reforzar el gobierno de la seguridad TIC en la Administración de la Junta de Andalucía y se centra, fundamentalmente, en introducir cambios en la organización corporativa de la seguridad TIC, potenciando la estructura de gobierno mediante la definición de atribuciones específicas a las Consejerías en relación con su propia seguridad y con la de las entidades vinculadas o dependientes de ellas, clarificando la aplicación del principio de función diferenciada y delimitando las funciones que deben desempeñar las distintas áreas implicadas en el mantenimiento de la seguridad, en línea con los perfiles con responsabilidad en seguridad definidos en la normativa reguladora del Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Consecuentemente, la novedad más significativa fue la sustitución del Responsable de Seguridad TIC tanto corporativo como de las Consejerías por una Unidad de Seguridad TIC corporativa de la Junta de Andalucía y en otra Unidad de Seguridad TIC por cada Consejería con funciones más definidas, cuya persona titular será la que asuma el papel, funciones y responsabilidades encomendados al Responsable de Seguridad por el Esquema Nacional de Seguridad. Solamente los entes instrumentales mantendrán la figura del Responsable de Seguridad TIC como puesto unipersonal y no como unidad. De acuerdo con el principio de función diferenciada la responsabilidad de la seguridad de los sistemas de tecnologías de la información y comunicaciones estará diferenciada de la responsabilidad sobre la prestación de servicios.

00141662

En la elaboración de esta Orden se ha tenido en cuenta, además de la normativa actualmente aplicable en materia de datos de carácter personal, el Reglamento 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), directamente aplicable a partir del 25 de mayo de 2018.

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 veinticinco artículos, distribuidos en tres capítulos, una disposición adicional y dos disposiciones finales.

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

El capítulo II se refiere a la política de seguridad TIC de la Consejería. En este capítulo se da cumplimiento en el ámbito de la Consejería de la Presidencia, Administración Local y Memoria Democrática a dos obligaciones en materia de seguridad TIC impuestas tanto por el Esquema Nacional de Seguridad como por la normativa reguladora de la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía.

Por un lado, establece la estructura de organización y gestión de la seguridad TIC de la Consejería. A este respecto, contiene la creación del Comité de Seguridad TIC, su composición, funciones y régimen de funcionamiento. Dispone la existencia en su seno de un Grupo de Respuesta a Incidentes en los Sistemas de Información para la toma urgente de decisiones en caso de contingencia grave que afecte a la seguridad de los sistemas de información críticos de la Consejería. También recoge el establecimiento de la Unidad de Seguridad TIC de la Consejería así como sus funciones y responsabilidades.

Por otro lado, aprueba el Documento de Política de Seguridad de la Consejería. Para ello define los roles o funciones de seguridad, prevé las normas para su desarrollo, establece los principios de la política de seguridad TIC de la Consejería, la gestión de riesgos, obligaciones del personal, y por último, refleja las obligaciones de auditoría de seguridad ya establecidas legalmente.

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, que aprueba el Reglamento General de Protección de Datos, que afectan directamente a la seguridad TIC. Entre ellos el principio de integridad y confidencialidad de los datos de carácter personal recogido en su artículo 5.1.f). que supone que 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.

Además de asumir la incidencia de los aspectos fundamentales del nuevo Reglamento General de Protección de Datos, recoge sus figuras fundamentales, como son el Responsable del Tratamiento, el Encargado del Tratamiento y el Delegado de Protección de Datos, en la política de seguridad TIC de la Consejería.

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. En cuanto a los principios de necesidad y eficacia, la Orden no hace sino desarrollar el artículo 10.1 del Decreto 1/2011, de 11 de enero, como estaba obligada, teniendo el rango normativo de Orden en cumplimiento de lo dispuesto en su apartado 2; cumple con el de proporcionalidad al desarrollar estrictamente con el mandato del Decreto, no imponiendo más obligaciones a la ciudadanía ni a la Administración que los establecidos en él y

00141662

regulando figuras necesarias para el cumplimiento de la finalidad perseguida; sobre el de seguridad jurídica, se han tenido en cuenta todas las normas europeas, estatales y autonómicas de aplicación; acerca del de transparencia, al tratarse de una disposición de organización interna no ha habido consulta previa ni trámite de audiencia a la ciudadanía, limitándose los informes a los internos de la Administración; y, por fin, es eficiente porque no sólo evita imponer cargas administrativas adicionales, sino que se limita a utilizar los recursos ya existentes para dar los servicios requeridos sin que suponga ningún incremento de gasto.

En su virtud, a propuesta de la Secretaría General Técnica de la Consejería, en uso de las atribuciones que me vienen conferidas por el artículo 26 de la Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía, los Decretos de la Presidenta 12/2017, de 8 de junio, de la Vicepresidencia y sobre reestructuración de Consejerías, 13/2017, de 8 de junio, de nombramiento de Consejero de la Presidencia, Administración Local y Memoria Democrática, y en el Decreto 204/2015, de 14 de julio, modificado por el Decreto 142/2017, de 29 de agosto, por el que se establece la estructura orgánica de la Consejería de la Presidencia y Administración Local y Memoria Democrática,

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 la Presidencia, Administración Local y Memoria Democrática, en adelante la Consejería, así como el marco organizativo y tecnológico de acuerdo con la normativa reguladora de la política de seguridad de las tecnologías de la información y comunicaciones de la Administración de la Junta de Andalucía, en el marco de la normativa reguladora del Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, en adelante ENS, y de la normativa en materia de protección de datos de carácter personal.

2. La presente Orden constituye el Documento de Política de Seguridad TIC de la Consejería de la Presidencia, Administración Local y Memoria Democrática.

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 la Presidencia, Administración Local y Memoria Democrática, 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 Administración General 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.

00141662

CAPÍTULO II

Política de Seguridad TIC

Artículo 3. Objetivos.

Son objetivos de la política de seguridad TIC:

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 4. Principios básicos.

Los principios básicos que regirán la política de seguridad TIC de la Consejería serán, además de los establecidos en la normativa reguladora de la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía y en el Esquema Nacional de Seguridad en el ámbito de la administración electrónica, 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 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.

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 de carácter personal: Los datos personales serán tratados de tal manera que se garantice una seguridad adecuada de

00141662

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 5. 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 Esquema Nacional de Seguridad en el ámbito de la administración electrónica, está compuesta por las siguientes figuras:

a) El Comité de Seguridad de las Tecnologías de la Información y Comunicaciones, en adelante Comité de Seguridad TIC, y el Grupo de Respuesta a Incidentes en los Sistemas de Información.

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 del Sistema.

e) Responsables del Servicio.

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 de carácter personal:

a) Responsables de los Tratamientos de datos de carácter personal.

b) Encargados de los Tratamientos de datos de carácter personal.

c) El Delegado de Protección de Datos, en adelante DPD.

Artículo 6. Creación del Comité de Seguridad de las Tecnologías de la Información y Comunicaciones.

1. Se crea el Comité de Seguridad de las Tecnologías de la Información y Comunicaciones de la Consejería de la Presidencia, Administración Local y Memoria Democrática, en adelante el Comité de Seguridad TIC.

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.

Artículo 7. 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 Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, y en la normativa reguladora de la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía y determinar la política de seguridad que se ha de emplear en la utilización de los medios electrónicos que permita la adecuada protección de la información.

2. En particular, le corresponde:

a) Aprobar el desarrollo de la política de seguridad TIC de segundo nivel, según lo previsto en el artículo 18.

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.

00141662

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

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 necesarios para ello. Especialmente, para asegurar que todos y cada uno de los miembros de la estructura de seguridad definida conozcan sus funciones y responsabilidades.

g) Nombrar un Grupo de Respuesta a Incidentes de Seguridad de la Información.

h) 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.

i) Promover y fomentar la divulgación y formación en cultura de la seguridad TIC, 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.

j) Velar porque 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.

k) 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.

l) Resolver los conflictos que puedan aparecer entre las diferentes personas responsables o entre diferentes áreas de la organización en materia de seguridad TIC.

m) 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 DPD.

n) Coordinar el Documento de Seguridad en los términos exigidos por la normativa de protección de datos de carácter personal.

Artículo 8. 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.

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

c) Vocalías: Las personas titulares de todos los órganos directivos centrales, la persona titular de la Coordinación General de la Secretaría General Técnica y la persona titular de la Coordinación de los Servicios Territoriales y Entidades Adscritas.

d) Secretaría: La persona titular de la Jefatura del Servicio de Informática, con voz y voto. En los casos de vacante, ausencia, enfermedad u otra causa legal, será sustituida por una persona funcionaria adscrita al Servicio de Informática, que designe la presidencia del Comité de Seguridad TIC.

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 podrán designar una persona que les sustituya en estas circunstancias entre personal funcionario que ocupen puestos de trabajo de nivel 28 o superior.

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

00141662

4. La persona titular de la Unidad de Seguridad TIC y la persona que ostente la condición de Delegado de Protección de Datos asistirán en calidad de asesores a las reuniones del Comité de Seguridad TIC, salvo que puntualmente se disponga lo contrario de forma expresa 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 9. Funcionamiento y régimen jurídico 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.

3. El Comité de Seguridad TIC se regirá por esta Orden, por la normativa reguladora de la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía, así como por el resto de normativa aplicable, como la reguladora del ENS y la normativa de protección de datos de carácter personal.

Artículo 10. Grupo de Respuesta a Incidentes en los Sistemas de la Información

1. El Comité de Seguridad TIC nombrará un Grupo de Respuesta a Incidentes de Seguridad de la Información, cuya función será la toma urgente de decisiones en caso de contingencia grave que afecte a la seguridad de los sistemas de información críticos de la Consejería. Será la persona titular de la Presidencia del Comité de Seguridad TIC quien determine la existencia de tales contingencias y las califique como graves. Las decisiones adoptadas por este grupo serán ratificadas por el Comité en su conjunto cuando sea necesario.

2. La composición mínima de este grupo será la siguiente:

a) La persona titular de la Presidencia del Comité de Seguridad TIC.

b) La persona titular de la Vicepresidencia del Comité de Seguridad TIC.

c) La persona titular de la Secretaría General de la Oficina del Portavoz del Gobierno

d) Las personas titulares de los órganos directivos centrales y periféricos que se vean afectados por el incidente.

e) La persona titular de la Coordinación General de la Secretaría General Técnica.

f) La persona titular de la Jefatura del Servicio de Informática.

3. En el ejercicio de las funciones del grupo participarán en calidad de asesores:

a) La persona responsable de la Unidad de Seguridad TIC.

b) La persona que ostente la condición de Delegado de Protección de Datos.

4. Su composición podrá ser modificada mediante acuerdo del Comité de Seguridad TIC.

5. Corresponde al Grupo de Respuesta a Incidentes de Seguridad de la Información, entre sus funciones, notificar a la autoridad competente en materia de seguridad de las redes y sistemas de información, concretamente a su equipo de respuesta a incidentes de seguridad informática (CSIRT o CERT), los incidentes de seguridad TIC, en los casos y en los términos que determine la normativa aplicable.

6. La notificación mencionada en el apartado anterior podrá realizarse bien directamente, bien a través de AndalucíaCERT o por el medio o procedimiento que disponga la política de seguridad de las tecnologías de la información y comunicaciones de la Junta de Andalucía que determine la Dirección General competente en materia de coordinación y ejecución de las políticas de seguridad de los sistemas de información

00141662

y telecomunicaciones de la Administración de la Junta de Andalucía o el Comité de Seguridad TIC corporativo de la Junta de Andalucía.

7. La Consejería estará integrada en el grupo atendido del Centro de Seguridad TIC AndalucíaCERT

Artículo 11. 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 la persona responsable de la citada Unidad entre personal funcionario al servicio de la Consejería por el Comité de Seguridad TIC de la misma.

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

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

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

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

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

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

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

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

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

Artículo 12. 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 Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Artículo 13. Responsables de la Información.

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

2. Las principales 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.

00141662

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

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

Artículo 14. Responsables de los Servicios.

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

2. Las principales 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.

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

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

Artículo 15. Responsables de los Sistemas.

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

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

3. Sus principales 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 porque 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) Creación, mantenimiento y actualización continua de 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 los Responsables de la Información y a los Responsables de los Servicios, en el proceso de la gestión de riesgos.

00141662

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.

Artículo 16. 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. En caso de conflicto prevalecerán las decisiones del Comité de Seguridad TIC adoptadas en sesión plenaria sobre las adoptadas por el Grupo de Respuesta a Incidentes de Seguridad de la Información.

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 de carácter personal prevalecerá la decisión que presente un mayor nivel de exigencia respecto a la protección de los datos de carácter personal.

Artículo 17. 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.

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

5. Cualquier persona que actúe bajo la autoridad del Responsable o del 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 siguiendo instrucciones del Responsable, salvo que se lo impida el ordenamiento jurídico comunitario, nacional o autonómico.

Artículo 18. 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 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.

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.

00141662

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 jefatura del Servicio de Informática o el Responsable del Sistema en el caso del artículo 15.2.

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.

La siguiente tabla resume el marco de desarrollo y la competencia para su aprobación:

Nivel	Documento	Aprueba
Primero	Política de seguridad	Persona titular de la Consejería de la Presidencia, Administración Local y Memoria Democrática
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 el Responsable del Sistema en el caso del artículo 15.2.

5. La Unidad de Seguridad TIC se encarga de la gestión de los documentos indicados, debiendo asegurar que ésta 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.

Artículo 19. 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 los 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 de carácter personal, 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. Los Responsables de la Información y de los Servicios son los responsables de aceptar los riesgos residuales calculados en el análisis sobre la información y los servicios, respectivamente, y de realizar su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.

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 al menos con periodicidad anual por parte de la Unidad de Seguridad TIC, que elevará un informe al Comité de Seguridad TIC.

Artículo 20. 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,

00141662

un persona 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.

Artículo 21. 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, y la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información, aprobada por Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública.

2. Los informes de auditoría serán presentados a la persona Responsable del Sistema competente, al Delegado de Protección de Datos, si afectara a estos, 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. 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 de protección de datos o medidas análogas de verificación, evaluación y valoración de seguridad de los tratamientos se realizarán de manera conjunta.

CAPÍTULO III

Protección de datos de carácter personal

Artículo 22. Incidencia de la normativa de protección de datos de carácter personal.

1. Todos los sistemas de información de la Consejería se ajustarán a lo exigido por el Reglamento 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, en adelante Reglamento General de Protección de Datos, y el resto de la normativa general o sectorial de protección de datos de carácter personal que sea de aplicación. Todos los tratamientos de datos de carácter personal, automatizados o no automatizados, se sujetarán a la citada norma cuando se encuentren dentro de su ámbito de aplicación.

2. En dicho ámbito cada Responsable del Tratamiento de datos de carácter personal aplicará las medidas técnicas y organizativas apropiadas a fin de garantizar y ser capaz de demostrar que los tratamientos de datos de carácter personal son conformes con dicha normativa, de acuerdo con el principio de responsabilidad proactiva, de conformidad con el artículo 24 del Reglamento General de Protección de Datos. En caso de conflicto con la normativa de seguridad prevalecerá el criterio que presente un mayor nivel de exigencia respecto a la protección de los datos de carácter personal.

3. Teniendo en cuenta el estado de la técnica, los costes de aplicación y la naturaleza, el alcance, el contexto y los fines del tratamiento de datos de carácter personal, así como 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, el Responsable y el Encargado del Tratamiento en el ámbito de aplicación de esta Orden, aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) La seudonimización y el cifrado de datos personales.

00141662

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.

4. Cuando sea probable que un tipo de tratamiento de datos personal, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el Responsable del Tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales, de conformidad con el artículo 32 del Reglamento General de Protección de Datos. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares. Para ello recabará el asesoramiento del Delegado de Protección de Datos.

5. El Responsable del Tratamiento llevará un registro de las actividades de tratamiento de datos de carácter personal efectuadas bajo su responsabilidad, de acuerdo con lo establecido en el artículo 35 del Reglamento General de Protección de Datos y el resto de normativa de datos de carácter personal aplicable. Cada Encargado 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.

6. En caso de violación de la seguridad de los datos personales, el 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, el Responsable del Tratamiento la comunicará al interesado sin dilación indebida. Dicha notificación y comunicación se atendrán a lo establecido en los artículos 33 y 34 del Reglamento General de Protección de Datos y el resto de normativa de datos de carácter personal aplicable.

7. 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 de la política de seguridad de las tecnologías de la información y comunicaciones de la Junta de Andalucía.

Artículo 23. Responsables de los Tratamientos de datos de carácter personal.

1. Los Responsables de los Tratamientos de datos de carácter personal en el ámbito de aplicación de esta Orden son las autoridades públicas que determinen los fines y medios de los tratamientos, de conformidad con el artículo 4.7 del Reglamento General de Protección de Datos.

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

Artículo 24. Encargados de los Tratamientos de datos de carácter personal.

1. Si los Responsables de los Tratamientos designaran a un Encargado del Tratamiento lo harán únicamente por cada tratamiento a un Encargado de Tratamiento que ofrezca garantías suficientes para aplicar las medidas técnicas y organizativas apropiadas para

00141662

que el tratamiento sea conforme al Reglamento General de Protección de Datos y garantice la protección de los derechos de las personas interesadas, de conformidad con el artículo 28 del Reglamento General de Protección de Datos.

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. Tanto el Responsable como el Encargado del Tratamiento deberá determinar claramente cuándo el tratamiento se realiza bajo su autoridad, conforme a lo establecido en el artículo 29 del Reglamento General de Protección de Datos y cuándo se realiza mediante un Encargado de Tratamiento sujeto a lo establecido en el artículo 28 de dicho Reglamento General de Protección de Datos.

Artículo 25. Delegado de Protección de Datos.

1. Existirá una persona que ostente la condición de Delegado de Protección de Datos a efectos de lo establecido en los artículos 37 y 38 del Reglamento General de Protección de Datos, para varios de los órganos y unidades administrativas de la Consejería de la Presidencia, Administración Local y Memoria Democrática que formen parte de Administración de la Junta de Andalucía, de conformidad con la posibilidad establecida en el artículo 37.3 de dicho Reglamento.

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

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

a) Ser consultado sobre la contratación, análisis, diseño, operación y mantenimiento de los tratamientos realizados sobre datos personales. También debe ser consultado sobre todo proyecto normativo que suponga un tratamiento de datos personales.

b) Asesorar sobre la confección de los modelos de formularios de recogida de datos personales.

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

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

e) Asesorar al Responsable del Tratamiento sobre la oportunidad y modo de notificar los incidentes de seguridad sobre datos de carácter personal a la autoridad de control correspondiente en materia de protección de datos de carácter personal.

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

00141662

Disposición adicional única. 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 la Unidad de Seguridad TIC, mediante la designación de su persona responsable y al nombramiento de los Responsables de la Información y de los Servicios.

Disposición final primera. 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 final segunda. Entrada en vigor.

La presente Orden entrará en vigor a partir del día siguiente al de su publicación en el Boletín Oficial de la Junta de Andalucía.

Sevilla, 30 de agosto de 2018

MANUEL JIMÉNEZ BARRIOS
Vicepresidente de la Junta de Andalucía
y Consejero de la Presidencia,
Administración Local y Memoria Democrática

00141662