1. Disposiciones generales

CONSEJERÍA DE IGUALDAD, POLÍTICAS SOCIALES Y CONCILIACIÓN

Orden de 25 de febrero 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 de carácter personal de la Consejería de Igualdad, Políticas Sociales y Conciliación.

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

Las Leyes 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, vienen a configurar un escenario en el que la tramitación electrónica debe constituir la actuación habitual de las Administraciones en sus múltiples vertientes de gestión interna, de relación con la ciudadanía y de relación de aquellas entre sí.

En concreto, la Ley 39/2015, de 1 de octubre, tiene como uno de sus objetivos centrales regular las relaciones entre las Administraciones y la ciudadanía y empresas, teniendo en cuenta el desarrollo de las tecnologías de la información y comunicación de los últimos años y cómo este afecta a las relaciones entre estos agentes. Pretende implantar una Administración totalmente electrónica, interconectada y transparente, mejorando la agilidad de los procedimientos administrativos y reduciendo los tiempos de tramitación. Por su parte, la Ley 40/2015, de 1 de octubre, procura dotar a nuestro sistema legal de una norma comprensiva del régimen jurídico de las Administraciones Públicas, regulando el funcionamiento interno de cada Administración y de las relaciones entre ellas.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (en adelante ENS), modificado mediante Real Decreto 951/2015, de 23 de octubre, tiene precisamente por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la Ley 40/2015, de 1 de octubre, y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada.

En lo referente a la protección de datos de carácter personal, resultan de aplicación, tanto el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante, RGPD), como la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

En cuanto al ámbito autonómico, el Estatuto de Autonomía para Andalucía, en su artículo 34, reconoce el derecho a acceder y usar las nuevas tecnologías y a participar activamente en la sociedad del conocimiento, la información y la comunicación, mediante los medios y recursos que la ley establezca. Asimismo, el artículo 58.1.2.º atribuye a la Comunidad Autónoma de Andalucía competencias exclusivas sobre el régimen de las nuevas tecnologías relacionadas con la Sociedad de la Información y del Conocimiento, en el marco de la legislación del Estado.

00170586

Por otro lado, la Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía, señala en su artículo 7.2 que los principios que rigen las relaciones que mantenga la Administración de la Junta de Andalucía con la ciudadanía y con otras Administraciones Públicas a través de redes abiertas de telecomunicación son los de simplificación y agilización de trámites, libre acceso, accesibilidad universal y confidencialidad en el tratamiento de la información, y de seguridad y autenticidad en orden a la identificación de las partes y el objeto de la comunicación. Para ello establece que estos sistemas deben cumplir con el requisito de existencia de medidas de seguridad que eviten la interceptación y alteración de las comunicaciones, así como los accesos no autorizados. En este mismo texto legal se abunda en materia de seguridad señalándose que los medios o soportes en que se almacenen los documentos electrónicos contarán con las medidas de seguridad que garanticen la integridad, protección y conservación de los documentos almacenados, así como la identificación de las personas usuarias y el control de acceso de los mismos.

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

La modificación del Decreto 1/2011, de 11 de enero, introdujo cambios en la organización corporativa de la seguridad de las Tecnologías de la Información y Comunicaciones (en adelante TIC), potenciando la estructura de gobierno mediante la definición de atribuciones específicas a las Consejerías en relación con su propia seguridad y con la de las entidades vinculadas o dependientes de ellas, clarificando la aplicación del principio de función diferenciada y delimitando las funciones que deben desempeñar las distintas áreas implicadas en el mantenimiento de la seguridad, en línea con los perfiles con responsabilidad en seguridad definidos en el ENS.

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

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

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

Además, en la elaboración y tramitación de la presente orden, se ha actuado conforme a los principios de buena regulación a los que se refiere el artículo 129.1 de la Ley 39/2015, de 1 de octubre. En cuanto a los principios de necesidad y eficacia, la orden no hace sino desarrollar el artículo 10.1 del Decreto 1/2011, de 11 de enero, como estaba obligada, teniendo el rango normativo de Orden en cumplimiento de lo dispuesto en su apartado 2; cumple con el de proporcionalidad al desarrollar estrictamente con el mandato del Decreto, no imponiendo más obligaciones a la ciudadanía ni a la Administración que los establecidos en él y regulando figuras necesarias para el cumplimiento de la finalidad perseguida; sobre el de seguridad jurídica, se han tenido en cuenta todas las normas

00170586

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 solo evita imponer cargas administrativas adicionales, sino que se limita a utilizar los recursos ya existentes para dar los servicios requeridos sin que suponga ningún incremento de gasto.

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

En su virtud, a propuesta de la Secretaría General Técnica de la Consejería de Igualdad, Políticas Sociales y Conciliación en uso de las atribuciones conferidas por los artículos 44.2 de la Ley 6/2006, de 24 de octubre, del Gobierno de la Comunidad Autónoma de Andalucía, y 26.2 a) de la Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía, y conforme a lo establecido en el Decreto 106/2019, de 12 de febrero, por el que se establece la estructura orgánica de la Consejería de Igualdad, Políticas Sociales y Conciliación, modificado por el Decreto 458/2019, de 23 de abril,

D I S P O N G O

Artículo 1. Objeto.

La presente orden tiene por objeto definir y regular la política de seguridad de las Tecnologías de la Información y las Comunicaciones en el ámbito de la Consejería de Igualdad, Políticas Sociales y Conciliación, en adelante política de seguridad TIC, que se ha de aplicar en el tratamiento de los activos de tecnologías de la información y comunicaciones de su titularidad o cuya gestión tenga encomendada.

Artículo 2. Ámbito de aplicación.

La orden será de aplicación a todos los sistemas de información que son responsabilidad de la Consejería de Igualdad, Políticas Sociales y Conciliación, utilizados por sus servicios centrales, periféricos y entidades vinculadas o dependientes de acuerdo con lo dispuesto en el Decreto por el que se establece la estructura orgánica de la misma. También será de aplicación a todas las personas que accedan a los sistemas de información así como a la propia información que sea gestionada por dicha Consejería, con independencia de cuál sea su destino, adscripción o relación con la misma.

Artículo 3. Objetivos, principios y definiciones.

Se asumen las definiciones, los objetivos y los principios, establecidos en los artículos 2, 4 y 5, respectivamente, 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, modificado por el Decreto 70/2017, de 6 de junio, circunscritos al ámbito competencial de los órganos contemplados en el ámbito de aplicación de esta norma.

Artículo 4. Contexto tecnológico y responsabilidad general.

1. La Consejería de Igualdad, Políticas Sociales y Conciliación depende de forma significativa de las Tecnologías de la Información y Comunicaciones, en adelante TIC, para alcanzar sus objetivos. En consecuencia, éstas deben ser administradas con diligencia, tomando las medidas adecuadas para protegerlas frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

00170586

2. La preservación de la seguridad TIC será considerada objetivo común de todas las personas al servicio de los órganos contemplados en el ámbito de aplicación de esta norma, así como a las personas que presten servicios como consecuencia de contrato administrativo suscrito por cualquiera de las anteriores, siendo éstas responsables del uso correcto de los activos TIC puestos a su disposición.

3. Todas las personas que presten servicios a la Consejería de Igualdad, Políticas Sociales y Conciliación tienen la obligación de conocer y cumplir, en sus respectivos ámbitos de actuación, la presente política de seguridad TIC, así como la normativa de seguridad que emana de la misma, siendo responsabilidad del Comité de Seguridad TIC de la Consejería de Igualdad, Políticas Sociales y Conciliación disponer los medios necesarios para que la información llegue a las personas interesadas.

4. Con carácter general, para el personal de la Consejería de Igualdad, Políticas Sociales y Conciliación, será de aplicación la normativa sobre conducta y uso aceptable de los recursos TIC de la Administración de la Junta de Andalucía vigente en cada momento.

5. La normativa sobre conducta y uso aceptable de los recursos TIC será trasladada convenientemente, en la medida en que pueda resultar necesario o recomendable, al clausulado de los contratos suscritos por la Consejería de Igualdad, Políticas Sociales y Conciliación.

Artículo 5. Marco normativo de la seguridad TIC.

Se asume como marco normativo 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.

Artículo 6. Estructura organizativa de la seguridad TIC.

1. La gestión de la seguridad de la información en un organismo va íntimamente ligada al establecimiento de una organización de seguridad. Dicha organización se establece mediante la identificación de las diferentes actividades y responsabilidades en materia de gestión de la seguridad y mediante su asignación formal a los agentes que correspondan, con arreglo al principio básico de función diferenciada recogido tanto en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS) como en la política de seguridad TIC de la Administración de la Junta de Andalucía.

2. Atendiendo a dicho principio, la estructura que se define en este documento diferencia tres grandes bloques de responsabilidad: la especificación de las necesidades y requisitos en materia de seguridad de la información; el desarrollo y explotación del sistema de información; la función de supervisión de la seguridad del sistema de información. En este sentido, los distintos bloques de responsabilidad mencionados quedarán distribuidos convenientemente, conforme a lo estipulado en el articulado de esta Orden, sobre los distintos agentes integrantes de la siguiente estructura organizativa a dos niveles:

a) En la Consejería de Igualdad, Políticas Sociales y Conciliación propiamente:

En relación con el ENS en el ámbito de la administración electrónica:

1. Comité de Seguridad TIC.
2. Responsables de la Información.
3. Responsables del Servicio.
4. Unidad de Seguridad TIC.
5. Responsable del Sistema.

00170586

En relación con la normativa de protección de datos de carácter personal:
1. Responsables de los tratamientos de datos de carácter personal.
2. Encargados/as de los tratamientos de datos de carácter personal.
3. Delegado/a de Protección de Datos.

b) En cada una de las entidades vinculadas o dependientes:
En relación con el ENS en el ámbito de la administración electrónica:
1. Comité de Seguridad TIC.
2. Responsables de la Información.
3. Responsables del Servicio.
4. Responsable de Seguridad TIC.
5. Responsable del Sistema.

En relación con la normativa de protección de datos de carácter personal:
1. Responsables de los tratamientos de datos de carácter personal.
2. Encargados/as de los tratamientos de datos de carácter personal.
3. Delegado/a de Protección de Datos.

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

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

Artículo 7. Comité de Seguridad TIC de la Consejería de Igualdad, Políticas Sociales y Conciliación.

1. Se crea el Comité de Seguridad TIC de la Consejería de Igualdad, Políticas Sociales y Conciliación como órgano colegiado de dirección y seguimiento en materia de seguridad de los activos TIC de los que la Consejería sea titular o cuya gestión tenga encomendada.

2. La composición del Comité de Seguridad TIC estará formado por:

a) La persona titular de la Viceconsejería, que ejercerá la Presidencia del Comité.

b) La persona titular de Secretaría General Técnica, que ejercerá la Vicepresidencia del Comité.

c) Las personas titulares de los órganos directivos centrales de la Consejería de Igualdad, Políticas Sociales y Conciliación que sean responsables de tratamientos, información o servicios y la persona titular de la Jefatura de Servicio competente en Sistemas de Información, que actuarán como Vocales.

d) La persona titular de la Jefatura del Servicio de Informática que además de actuar como Vocal, ejercerá la Secretaría del Comité.

e) La persona que ostente la condición de Delegado/a de Protección de Datos y la persona titular de la Unidad de Seguridad TIC, en calidad de vocalías asesoras con voz y sin voto.

3. El Comité de Seguridad TIC podrá recabar de personal técnico especializado, propio o externo, la información pertinente para la toma de decisiones.

4. En caso de vacante, ausencia, enfermedad u otras causas legales, de alguna de las personas miembros del Comité el régimen de suplencias será el siguiente:

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, de acuerdo con lo dispuesto en el régimen de suplencias establecido en el artículo 13 de la Ley 40/2015, de 1 de octubre del Régimen Jurídico del Sector Público.

00170586

5. Serán funciones propias del Comité de Seguridad TIC:

a) Definición, aprobación y seguimiento de los objetivos, iniciativas y planes estratégicos en materia de seguridad TIC.

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

c) Nombramiento de la Unidad de Seguridad TIC de la Consejería.

d) Elevación de propuestas de revisión de la política de seguridad TIC, de directrices y normas de seguridad de la Consejería, o de revisión del marco normativo de seguridad TIC de la Administración de la Junta de Andalucía, a los órganos competentes para su reglamentaria tramitación.

e) Aprobación del desarrollo de la normativa de seguridad TIC de segundo nivel de la Consejería, según el artículo 18.1 de la presente Orden.

f) Establecimiento de directrices comunes y supervisión del cumplimiento de la normativa en materia de seguridad TIC.

g) Supervisión del nivel de riesgo y toma de decisiones en la respuesta a incidentes de seguridad TIC que afecten a los activos TIC.

h) Coordinación con los Comités de Seguridad TIC de las entidades instrumentales vinculadas o dependientes de la Consejería.

i) Promoción de formación, entrenamiento y concienciación sobre las medidas legales y organizativas relativas a la seguridad TIC entre el personal de la Consejería.

j) Impulsar la determinación de los niveles de seguridad de la información tratada, en la que se valorarán los impactos que tendrían los incidentes que afectaran a la seguridad de la información, todo ello con la participación de los Responsables de la Información y de los Tratamientos correspondientes y de la Unidad de Seguridad TIC.

k) Impulsar los preceptivos análisis de riesgos, junto a los Responsables de la Información, Servicio y Tratamientos que correspondan, contando con la participación de la Unidad de Seguridad TIC.

l) Coordinar la aceptación de los riesgos residuales por sus personas responsables correspondientes respecto de la Información, Servicio y Tratamientos de su competencia, obtenidos en el análisis de riesgos.

m) Fomentar el establecimiento de mecanismos de comunicación con otros agentes especializados en esta materia.

6. La Presidencia del Comité de Seguridad TIC ostenta la representación del Comité de Seguridad TIC correspondiéndole:

- Acordar la convocatoria de las reuniones ordinarias y extraordinarias y establecer el orden del día de las mismas, a partir de las peticiones de los demás miembros.
- Presidir las reuniones, moderar los debates y suspenderlos por causas justificadas.
- Dirimir con su voto de calidad los empates en votaciones para la adopción de acuerdos.
- Certificar los acuerdos del Comité.

7. La Secretaría realiza las convocatorias de las reuniones por orden de la Presidencia del Comité, así como las citaciones al resto de miembros del Comité. También se encarga de elaborar las actas de las reuniones y los acuerdos adoptados.

8. Funcionamiento del Comité de Seguridad TIC de la Consejería.

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

El Comité de Seguridad TIC se reunirá previa convocatoria con carácter ordinario al menos una vez al año y, con carácter extraordinario, por acuerdo de la persona titular de la Presidencia, a iniciativa propia o a propuesta de alguno de sus miembros por medio electrónico, dirigido a la Presidencia con una antelación mínima de 48 horas a la fecha de la convocatoria.

00170586

El Comité se podrá constituir, convocar, celebrar sus sesiones, adoptar acuerdos y remitir actas, tanto de forma presencial como utilizando redes de comunicación a distancia, con las medidas adecuadas que garanticen la identidad de las personas comunicantes y la autenticidad de la información entre ellas transmitida.

El quorum necesario para la celebración de una reunión del Comité es la mitad más uno de los miembros que componen el Comité, siendo obligatoria la presencia de la Presidencia o suplente en su caso, y al menos una, de entre la persona que ostente la condición de Delegado de Protección de Datos o persona responsable de la Unidad de Seguridad TIC.

Los miembros del Comité de Seguridad TIC podrán individual o colectivamente, proponer a la Presidencia de forma motivada, la inclusión de determinados asuntos en el orden del día de una reunión ordinaria. La propuesta deberá realizarse por medio electrónico, dirigido a la Presidencia, con una antelación mínima de 10 días laborables siempre que la reunión no tenga un carácter urgente, en cuyo caso se requerirá una antelación mínima de 8 horas.

Las propuestas de acuerdos del Comité de Seguridad TIC serán sometidas a votación y estos se adoptarán por mayoría simple de los miembros presentes en la reunión.

En caso de empate, se realizará una nueva votación, y si este persistiera, decidirá el voto de calidad de la Presidencia.

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

Artículo 8. Responsables de la Información y Responsables del Servicio.

1. Las personas Responsables de la Información y del Servicio serán las personas titulares de los órganos directivos que decidan sobre la finalidad, contenido y uso de la información tratada o sobre las características del servicio a prestar.

2. En cumplimiento del artículo 10.4 del Decreto 1/2011, de 11 de enero, los deberes y responsabilidades principales de las personas Responsables descritas en el apartado 1, dentro de su ámbito de actuación y sin perjuicio de otras previstas en el ENS y la guía de seguridad CCN-STIC-801, son los siguientes:

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

b) Proporcionar la información necesaria a la Unidad de Seguridad TIC, para realizar los preceptivos análisis de riesgos, con la finalidad de establecer las salvaguardas a implantar. Para ello, contarán con la ayuda de la persona Responsable del Sistema, en su caso.

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

3. La designación y renovación de estas personas Responsables, se realiza por Orden de la persona titular de la Consejería.

Artículo 9. Unidad de Seguridad TIC de la Consejería de Igualdad, Políticas Sociales y Conciliación y Responsable de Seguridad TIC.

1. En virtud del artículo 11.1 del Decreto 1/2011, de 11 de enero, la Consejería contará con una Unidad de Seguridad TIC, garantizando el cumplimiento del 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.

00170586

2. La designación o renovación de la persona responsable de la Unidad de Seguridad TIC de la Consejería se realizará entre el personal funcionario del Cuerpo A.1 de la Administración General de la Junta de Andalucía adscrito a Secretaría General Técnica, mediante Acuerdo del Comité de Seguridad TIC de este organismo.

3. La Unidad de Seguridad TIC de la Consejería tendrá las siguientes atribuciones, de acuerdo con lo dispuesto en el artículo 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 este.

b) Diseño y ejecución de los programas de actuación propios de la Consejería, incluyendo, entre otros, planes directores de seguridad, proyectos de desarrollo normativo, auditorias 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 procedimiental, operacional y medidas técnicas de protección de los datos, aplicaciones y sistemas de la Consejería.

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

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

g) Coordinación, dirección y seguimiento de la actividad en materia de seguridad TIC de las entidades vinculadas o dependientes de la Consejería, a partir del momento en que se apruebe la políticas 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 depnenda funcional u orgánicamente.

4. La persona responsable de la Unidad de Seguridad TIC de la Consejería tendrá la condición de Responsable de Seguridad y, en virtud de los artículos 10.4 y 11.3 del Decreto 1/2011, de 11 de enero, la presente política de seguridad establece que le corresponderán los deberes y responsabilidades en los términos recogidos en el ENS y la guía de seguridad CCN-STIC-801. En concreto, le corresponde lo establecido en los artículos 10, 18, 27 y 34 sin perjuicio de otras funciones que pudieran corresponderle como Responsable de Seguridad.

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

Artículo 10. Responsable del Sistema.

1. La figura de Responsable del Sistema, entendiéndose como tal desde la perspectiva del ENS, de cada sistema de información que se encuentre albergado en

00170586

los servidores corporativos de la Consejería, será asumida por una persona funcionaria de la Administración General de la Junta de Andalucía adscrita al Servicio competente en Sistemas de Información, designada al efecto por la persona titular de la Jefatura de Servicio, que se encargará de desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida. Para cada sistema de información deberá existir una persona Responsable del Sistema, siendo posible que una misma persona sea responsable de varios sistemas.

2. En virtud del artículo 10.4 del Decreto 1/2011, de 11 de enero, la presente política de seguridad establece que los deberes y responsabilidades de este perfil de responsabilidad serán los previstos en el ENS y la guía de seguridad CCN-STIC-801 para la figura de Responsable del Sistema. En concreto, le corresponde lo establecido en los artículos 10, 34, y en el Anexo III del ENS.

3. La designación y renovación de la persona Responsable de Sistema, se realizará mediante resolución del órgano directivo competente en la aplicación de las TIC de la Consejería. En aquéllos sistemas de información cuya implantación, explotación y mantenimiento se haga en otros organismos de la Administración de la Junta de Andalucía o en entidades que no pertenezcan a dicha Administración, será nombrada o renovada por las personas Responsables de la Información o Responsables del Servicio correspondientes y se designará mediante resolución.

Artículo 11. Delegado de Protección de Datos de la Consejería de Igualdad, Políticas Sociales y Conciliación.

1. La figura de Delegado/a de Protección de Datos, en los términos establecidos en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante, RGPD), y por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, será asumida por una persona entre el personal funcionario de la Consejería del Cuerpo A.1 de la Administración General de la Junta de Andalucía, con adscripción a un órgano con competencias y funciones de carácter horizontal.

2. El nombramiento o renovación de la figura de Delegado/a de Protección de Datos se realizará mediante resolución de la persona titular de la Viceconsejería. No podrá ser removida ni sancionada por desempeñar sus funciones, salvo que incurriera en dolo o negligencia grave en su ejercicio.

3. La figura de Delegado/a de Protección de Datos velará por la elaboración y mantenimiento de un Registro de Actividades de Tratamiento de datos de carácter personal, con indicación expresa de las personas u órganos que asumen la figura de Responsable de Tratamiento, Encargado/a del Tratamiento y resto de requisitos exigidos por el art. 30 del RGPD. Dicho Registro se entregará actualizado, al Comité de Seguridad TIC de la Consejería en cada una de sus reuniones, con indicación de aquellas deficiencias o faltas de información que se produzcan, de modo que el Comité disponga de información completa y pueda arbitrar los mecanismos necesarios para la subsanación de las deficiencias o faltas de información.

Artículo 12. Responsables de los Tratamientos de datos de carácter personal.

1. La figura de 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 RGPD.

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 de 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.

00170586

3. La designación y renovación de estas personas Responsables se realizará por Orden de la persona titular de la Consejería.

Artículo 13. Encargados/as de los Tratamientos de datos de carácter personal.

1. Si las personas Responsables de los Tratamientos designaran a un/a Encargado/a del Tratamiento, lo harán únicamente por cada tratamiento al objeto de ofrecer garantías suficientes para aplicar las medidas técnicas y organizativas apropiadas para que el tratamiento sea conforme al RGPD y garantice la protección de los derechos de las personas interesadas, de conformidad con el artículo 28 del RGPD.

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

3. Tanto la persona Responsable del Tratamiento como la Encargada del mismo, deberán determinar claramente cuándo el tratamiento se realiza bajo su autoridad, conforme a lo establecido en el artículo 29 del RGPD y cuándo se realiza mediante un encargo de Tratamiento, que se regirá por un contrato u otro acto jurídico de acuerdo a lo establecido en el artículo 28 de dicho Reglamento.

Artículo 14. Estructura organizativa en entidades vinculadas o dependientes.

1. De acuerdo con el artículo 6.2.b) del Decreto 1/2011, de 11 de enero, la organización para la gestión de la seguridad TIC en las entidades vinculadas o dependientes de la Consejería de Igualdad, Políticas Sociales y Conciliación se conforma mediante la siguiente estructura:

a) Comité de Seguridad TIC.
b) Responsables de la Información.
c) Responsables del Servicio.
d) Responsable de Seguridad TIC.
e) Responsable del Sistema.

2. En función de las necesidades y circunstancias de la organización, las funciones de algunas de estas figuras podrá recaer sobre una misma persona, unidad o departamento.

3. La responsabilidad de la conformación y designación de estas figuras en las entidades vinculadas o dependientes recaerá sobre las propias entidades.

4. El Comité de Seguridad TIC de las entidades vinculadas o dependientes es un órgano colegiado de dirección y seguimiento en materia de seguridad de los activos TIC de los que la entidad sea titular o cuya gestión tenga encomendada. Las atribuciones de este Comité de Seguridad TIC podrán ser asumidas por el máximo órgano de dirección de la entidad, debiendo especificarse tal extremo, en su caso.

5. Las entidades vinculadas o dependientes contarán al menos con una persona Responsable de Seguridad TIC que será nombrada por el Comité de Seguridad TIC de las mismas y que tendrá las atribuciones previstas en el artículo 11.2 del Decreto 1/2011, de 11 de enero. Tendrá la condición de Responsable de Seguridad en los términos establecidos en el ENS.

En caso de que fuesen varias las personas designadas, la persona Responsable de Seguridad TIC tendrá atribuciones de coordinación y dirección de la labor desempeñada por el resto de personas responsables de seguridad designadas.

6. Los nombramientos realizados para los distintos perfiles de la estructura organizativa de seguridad TIC en las entidades vinculadas o dependientes deberán comunicarse al Comité de Seguridad TIC de la Consejería.

Artículo 15. Resolución de conflictos.

Los conflictos entre las diferentes unidades u órganos responsables que componen la estructura organizativa de la política de seguridad TIC, serán resueltos por el órgano superior jerárquico común. En su defecto, prevalecerá la decisión del Comité de Seguridad TIC.

00170586

Artículo 16. Datos de carácter personal.

1. Para el tratamiento de datos de carácter personal en los sistemas de información se seguirá en todo momento lo establecido en el RGPD, así como lo establecido en la legislación nacional y autonómica vigente en cada momento en relación con esta materia.

2. La seguridad de los datos de carácter personal se basará en criterios de reducción del riesgo dependiendo de la naturaleza y tratamientos de los mismos. Cada persona 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 la normativa mencionada en el apartado anterior.

3. Para el cumplimiento de la obligación de disponer de un Registro de Actividades de Tratamiento, se estará a lo indicado en el artículo 11.3 de esta orden.

Artículo 17. Gestión de riesgos.

1. La gestión de riesgos debe realizarse de manera continua sobre el sistema de información, conforme a los principios de gestión de la seguridad basada en los riesgos y reevaluación periódica. Para ello, se deben implementar las medidas mínimas de seguridad determinadas por el ENS así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos que cumpla los requisitos del ENS y del RGPD.

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

3. Las personas Responsables de la Información y del Servicio son los responsables de aceptar los riesgos residuales calculados en el análisis de riesgos sobre la información y los servicios, respectivamente, así como de realizar su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.

4. El Comité de Seguridad TIC es responsable de realizar un seguimiento de los principales riesgos residuales asumidos por la Consejería y de recomendar posibles actuaciones respecto de ellos.

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

6. El proceso de gestión de riesgos comprende las fases de identificación y valoración de informaciones y servicios esenciales prestados, categorización de los sistemas, análisis de riesgos y selección de medidas de seguridad a aplicar, las cuales deberán ser proporcionales a los riesgos y estar justificadas. Este análisis deberá revisarse cada año por parte de la Unidad de Seguridad TIC, que elevará el correspondiente informe al Comité de Seguridad TIC.

7. Para realizar el análisis de riesgos se utilizará la metodología de análisis y gestión de riesgos de los sistemas de información MAGERIT, aprobada por el Consejo Superior de Administración Electrónica, y las herramientas que la apliquen, entre ellas PILAR, desarrollada por el Centro Criptológico Nacional.

Artículo 18. Desarrollo normativo de la seguridad TIC.

1. La normativa sobre seguridad TIC es de obligado cumplimiento y se desarrollará en tres niveles, según el ámbito de aplicación y nivel de detalle técnico, de manera que lo establecido para un determinado nivel de desarrollo se fundamente en lo establecido para el nivel superior. Dichos niveles de desarrollo normativo son los siguientes:

a) Primer nivel normativo: política de seguridad TIC, constituido por la presente Orden y demás directrices y normas generales de seguridad TIC.

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

00170586

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

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 Igualdad, Políticas Sociales y Conciliación
Segundo	Normas de seguridad	Comité de Seguridad TIC
Tercero	Procedimientos	Persona titular de la Secretaría General Técnica

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

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

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

Artículo 19. Gestión de incidentes de seguridad y de la continuidad.

1. La Consejería deberá estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, según los términos previstos en el artículo 7 del ENS y en la Resolución de 13 de julio de 2018, de la Dirección General de Telecomunicaciones y Sociedad de la Información, por la que se establecen normas sobre gestión de incidentes de seguridad TIC.

2. El Comité de Seguridad TIC deberá aprobar y revisar periódicamente un plan para mantener la continuidad de los procesos y sistemas críticos y garantizar su recuperación en caso de desastre. La finalidad de este plan es reducir el tiempo de indisponibilidad a niveles aceptables mediante la combinación de controles de carácter organizativo, tecnológico y procedimental tanto preventivos como de recuperación.

3. A los efectos de una mejor gestión de los incidentes, se actuará de forma coordinada con AndalucíaCERT, como centro experto para la gestión de la seguridad TIC de la Junta de Andalucía.

Artículo 20. Formación y concienciación en seguridad TIC.

Anualmente se desarrollarán actividades de formación y concienciación en seguridad TIC destinadas a las personas empleadas públicas de los órganos contemplados en el ámbito de aplicación de esta norma. Entre tales actividades se incluirán las de difusión de esta política de seguridad TIC y de su desarrollo normativo.

Artículo 21. 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 directivo de la Consejería utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta política de seguridad TIC

00170586

y de la normativa de seguridad TIC que ataña a dichos servicios o información así como al personal adscrito a dichos terceros. Los terceros quedarán sujetos, 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 estos terceros de sus propios procedimientos operativos para satisfacerla. Se establecerán mecanismos de comunicación con otros agentes especializados en esta materia, en coordinación con la Unidad de seguridad TIC corporativa para los agentes externos a la Junta y resolución de incidencias.

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 o de la persona Responsable de Seguridad TIC en el supuesto que afecte a entidades vinculadas o dependientes, que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por las personas Responsables de la Información y del Servicio afectados antes de proseguir en la relación con la tercera parte.

Artículo 22. Auditorías y conformidad con la normativa.

1. La Consejería manifiesta el compromiso de auditar los sistemas de información de forma periódica con objeto de revisar el cumplimiento normativo vigente.

2. Los sistemas de información de la Consejería serán objeto, al menos cada dos años, de una auditoría regular ordinaria interna o externa que verifique el cumplimiento de los requisitos del ENS y de cualquier otra norma que requiera la realización de auditorías periódicas. La Unidad de Seguridad TIC realizará o, en su caso, coordinará, estas actividades de auditoría.

3. Con carácter extraordinario, deberá realizarse dicha auditoría siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad requeridas.

4. Los informes de auditoría serán presentados a la persona Responsable del Sistema, a la que desempeñe el cargo de Delegado/a de Protección de Datos si afectara a éstos, y a la persona responsable de la Unidad de Seguridad TIC, siendo ésta última quien deberá analizar dichos informes y presentar sus conclusiones a la persona Responsable del Sistema para que éste adopte las medidas correctoras adecuadas.

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

A efectos de coordinación, obtención de asesoramiento e intercambio de experiencias para la mejora continua de la gestión de la seguridad de la información, el Comité de Seguridad TIC fomentará el establecimiento de mecanismos de comunicación con otros agentes especializados en esta materia, en coordinación con la Unidad de Seguridad TIC Corporativa para los agentes externos a la Junta de Andalucía. Estos mecanismo podrían consistir en la celebración de encuentros, jornadas o reuniones con otros organismos públicos y grupos de interés. En especial, se contemplarán los siguientes:

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

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

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

d) Secretaría General de Regeneración, Racionalización y Transparencia, como órgano directivo competente en la coordinación y seguimiento del cumplimiento de la normativa aplicable en materia de protección de datos.

00170586

e) AndalucíaCERT.

f) 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.

g) Agencia Española de Protección de Datos (AEPD).

h) Instituto Nacional de Ciberseguridad (INCIBE).

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

Artículo 24. Actualización permanente y revisiones periódicas.

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

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

Artículo 25. Difusión de la política de seguridad TIC.

A los efectos de su mejor difusión entre el personal de la organización y de otras partes interesadas, la presente política de seguridad TIC se publicará y divulgará, además de en el Boletín Oficial de la Junta de Andalucía, a través de los medios que se establezcan por el Comité de Seguridad TIC.

Disposición adicional primera. Constitución del Comité de Seguridad TIC.

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

Disposición adicional segunda. Desarrollo y ejecución.

Se habilita a la persona titular de la Secretaría General Técnica para dictar cuantas instrucciones sean necesarias para la ejecución y desarrollo de lo establecido en la presente 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, 25 de febrero de 2020

ROCÍO RUIZ DOMÍNGUEZ
Consejera de Igualdad, Políticas Sociales
y Conciliación

00170586