1. Disposiciones generales

CONSEJERÍA DE EDUCACIÓN Y DEPORTE

Orden de 3 de diciembre de 2020, por la que se establece la política de seguridad de las tecnologías de la información y comunicaciones de la Consejería de Educación y Deporte.

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

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

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

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

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

En concreto, la Ley 39/2015, de 1 de octubre, tiene como uno de sus objetivos centrales regular las relaciones entre las Administraciones, la ciudadanía y las empresas, teniendo en cuenta el desarrollo de las tecnologías de la información y la comunicación de los últimos años y cómo este afecta a las relaciones entre estos agentes. Pretende implantar

00182973

una Administración totalmente electrónica, interconectada y transparente, mejorando la agilidad de los procedimientos administrativos y reduciendo los tiempos de tramitación. Por su parte, la Ley 40/2015, de 1 de octubre, procura dotar a nuestro sistema legal de una norma comprensiva del régimen jurídico de las Administraciones Públicas, regulando el funcionamiento interno de cada Administración y de las relaciones entre ellas.

Para el desarrollo de esta política de seguridad de las tecnologías de la información y las comunicaciones se ha seguido lo indicado en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de Protección de Datos) , así como y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales; en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, y su modificación parcial mediante Real Decreto 951/2015, de 23 de octubre; en el Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía; y en la Orden de 9 de junio de 2016, de la Consejería de Empleo, Empresa y Comercio, por la que se efectúa el desarrollo de la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía.

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

La Consejería de Educación y Deporte ha venido desarrollando durante años un conjunto de actuaciones dirigidas a garantizar una protección adecuada de la información y de los servicios, en el marco de la Política de Seguridad de Información regulada en la Orden de 11 de febrero de 2008 por la que se crea el Comité de Seguridad y se aprueba el Documento de Política de Seguridad de la Información de la Consejería.

Esta política de seguridad renueva el compromiso de la Consejería de Educación y Deporte con la seguridad de los sistemas de información, establecido por la Orden de 11 de febrero de 2008, definiendo los objetivos y criterios básicos para el tratamiento de la información y sentando los pilares del marco normativo de seguridad en la Consejería y la estructura organizativa y de gestión que velará por su cumplimiento.

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

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 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

00182973

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 Secretaria General Técnica de la Consejería, en uso de las atribuciones que me vienen conferidas por el artículo 44.2 de la Ley 6/2006, de 24 de octubre, del Gobierno de la Comunidad Autónoma de Andalucía, y conforme a la habilitación del artículo 10.2 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,

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, TIC), en el ámbito de la Consejería de Educación y Deporte, (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, 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 Educación y Deporte.

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, 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, 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

CAPÍTULO II

Política de Seguridad TIC

Artículo 3. Objetivos, principios y definiciones.

1. La misión de la Consejería se corresponde con las competencias atribuidas en el artículo 1 del Decreto 102/2019, de 12 de febrero, por el que se establece la estructura orgánica de la Consejería de Educación y Deporte.

00182973

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

Artículo 4. Marco regulador.

1. La Consejería asume como marco regulador general el definido, en virtud de la Disposición adicional primera del Decreto 1/2011, de enero, por la Consejería competente en materia de coordinación y ejecución de las políticas de seguridad de los sistemas de información y telecomunicaciones. Todo ello sin perjuicio de otra normativa aplicable a esta Consejería en virtud de su naturaleza legal y sus competencias.

2. La Consejería podrá ampliar y desarrollar el marco regulador en los términos previstos en el artículo 16 de esta orden, en base a la letra a) del apartado 1 de la disposición adicional primera del Decreto 1/2011, de 11 de enero.

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.

b) Unidad de Seguridad TIC.

c) Responsables de la Información y del Servicio.

d) Responsables del Sistema.

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 o la Delegada de Protección de Datos.

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 Educación y Deporte, en adelante el Comité de Seguridad TIC.

2. El Comité de Seguridad TIC actuará como órgano no colegiado 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.

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.

00182973

c) Definir, aprobar y realizar el seguimiento de los objetivos, iniciativas y planes estratégicos en materia de seguridad TIC.

d) 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.

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

f) 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.

g) 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.

h) Nombrar la Unidad de Seguridad TIC de la Consejería designando a su persona responsable.

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.

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 Delegado de protección de datos.

n) Elevar las propuestas de revisión de la Política de Seguridad TIC de la Consejería o de revisión del marco regulador de seguridad TIC de la Junta de Andalucía, a los órganos competentes para su reglamentaria tramitación.

ñ) Aprobar y revisar periódicamente un plan para mantener la continuidad TIC de los procesos y sistemas críticos y garantizar su recuperación en caso de un incidente que afecte gravemente a su disponibilidad.

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:

1.º Las personas titulares de todos los órganos directivos centrales, o las designadas por éstas entre el personal funcionario a su servicio.

2.º La persona o personas titulares de las unidades administrativas que lleven a cabo la planificación, diseño y ejecución de las actividades necesarias para la construcción, operación y mantenimiento de los sistemas de información de la Consejería.

3.º La persona que ejerza las funciones de dirección de cada entidad vinculada o dependiente, o la designada por ésta entre el personal a su servicio.

4.º La persona a la que se asignen las funciones de Delegado de Protección de Datos.

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

00182973

2. El Comité de Seguridad establecerá un régimen de suplencias en caso de que las personas titulares no puedan acudir a las reuniones del mismo.

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.

4. 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.

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. 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 de la Consejería tendrá las atribuciones que establece el artículo 11.1 del Decreto 1/2011, de 11 de enero.

Artículo 11. 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 12. Responsable de la información.

1. La persona en quien recaerá la figura de Responsable de Información será la persona titular del órgano directivo que decida sobre la finalidad, contenido y uso de la información, así como la que determine los niveles de seguridad dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad.

2. A los efectos previstos en la normativa de Protección de Datos Personales, la persona Responsable de la Información tendrá asimismo, respecto de los datos personales contenidos en la información incluida en su ámbito de actuación, la consideración de Responsable del Tratamiento.

3 En virtud del artículo 10.4 del Decreto 1/2011, de 11 de enero, los deberes y responsabilidades principales de este perfil de responsabilidad, dentro de su ámbito de actuación y sin perjuicio de otras previstas en el Esquema Nacional de Seguridad, son los siguientes:

00182973

a) Ayudar a determinar los requisitos de seguridad de la información, identificando los niveles de seguridad de la información 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 contará con la ayuda de la persona Responsable del Sistema (o los responsables si hubiere varios).

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

4 El nombramiento o renovación de esta figura responsable se realiza en virtud de la presente política de seguridad TIC, y conservarán su condición mientras ostenten el cargo que haya determinado su nombramiento.

Artículo 13. Responsable del servicio.

1. La persona en quien recaerá la figura de Responsable del servicio será la persona titular del órgano directivo que decida sobre las características del servicio a prestar, así como la que determine los niveles de seguridad dentro del marco establecido en el anexo I del Esquema Nacional de Seguridad.

2 En virtud del artículo 10.4 del Decreto 1/2011, de 11 de enero, los deberes y responsabilidades principales de este perfil de responsabilidad, dentro de su ámbito de actuación y sin perjuicio de otras previstas en el Esquema Nacional de Seguridad, son los siguientes:

a) Ayudar a determinar los requisitos de los servicios a prestar, identificando los niveles de seguridad 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 contará con la ayuda de la persona Responsable del Sistema (o los responsables si hubiere varios).

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

3 El nombramiento o renovación de esta figura responsable se realiza en virtud de la presente política de seguridad TIC, y conservarán su condición mientras ostenten el cargo que haya determinado su nombramiento.

Artículo 14. Responsables de los Sistemas.

1. Responsables de los Sistemas serán las personas titulares de las unidades administrativas de la Secretaría General Técnica que lleven a cabo la planificación, diseño y ejecución de las actividades necesarias para la construcción, operación y mantenimiento de los sistemas de información de la Consejería.

2. En el caso de los Sistemas que no dependan de las Unidades Administrativas anteriores, 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, la operación y el mantenimiento de los sistemas de información durante todo su ciclo de vida, así como las especificaciones de los mismos, la instalación y la 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.

00182973

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 las personas Responsables de la Información y a las personas Responsables de los Servicios, en el proceso de la gestión de riesgos.

h) Suspender el manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con las personas Responsables de la Información afectada, del Servicio afectado y con la Unidad de Seguridad TIC, antes de ser ejecutada.

Artículo 15. Resolución de conflictos.

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

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

Artículo 16. 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. 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.

3. 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.

4. Cualquier persona que actúe bajo la autoridad de la persona Responsable o de la persona Encargada de un Tratamiento de datos personales en el ámbito de aplicación de esta orden y tenga acceso a datos personales solo tratará dichos datos siguiendo instrucciones del Responsable.

Artículo 17. Desarrollo de la política de seguridad de la información.

1. La política de seguridad se desarrollara teniendo en cuenta los siguientes requisitos mínimos:

a) Organización e implantación del proceso de seguridad.

b) Análisis y gestión de los riesgos.

c) Gestión de personal.

d) Profesionalidad.

e) Autorización y control de los accesos.

f) Protección de las instalaciones.

00182973

g) Adquisición de productos.
h) Seguridad por defecto.
i) Integridad y actualización del sistema.
j) Protección de la información almacenada y en tránsito.
k) Prevención ante otros sistemas de información interconectados.
l) Registro de actividad.
m) Incidentes de seguridad.
n) Continuidad de la actividad.
ñ) Mejora continua del proceso de seguridad.

2. Las medidas sobre la seguridad TIC, de obligado cumplimiento, se desarrollarán en tres niveles con diferente ámbito de aplicación, detalle técnico y obligatoriedad de cumplimiento, pero de manera que cada elemento de desarrollo se fundamente en el nivel superior.

3. 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.

4. Los niveles de desarrollo son los siguientes:

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

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

c) Tercer nivel: Procedimientos y documentación técnica. Describen las acciones a realizar, de una manera más específica, en un proceso relacionado con la seguridad siendo dependientes de las normas de seguridad, así todo tipo de documentación técnica o especializada que se considere necesario para completar y facilitar el desarrollo de las medidas de seguridad . Los procedimientos y documentación deben ser aprobados por la persona responsable del Sistema correspondiente.

5. 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 Educación y Deporte
Segundo	Normas de seguridad	Comité de Seguridad TIC
Tercero	Procedimientos y documentación técnica	La persona responsable del sistema correspondiente

6. La Unidad de Seguridad TIC se encarga de la gestión de los documentos indicados, debiendo asegurar que esta sea completa y proporcione información suficiente para definir las necesidades de protección de la información y los activos asociados a la misma en el ámbito de la Consejería.

Artículo 18. Gestión de riesgos.

1. La gestión de riesgos deberá realizarse de manera continua sobre los sistemas 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 o las Responsables de la Información y de los Servicios, siendo la Unidad de Seguridad TIC la encargada de supervisar los análisis de riesgos y proponer las medidas de seguridad a aplicar.

00182973

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. Las personas Responsables de la Información y de los Servicios son las 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 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 Esquema Nacional de Seguridad. La Consejería adoptará las medidas en el ámbito de la gestión de incidentes de seguridad establecidas 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. La Consejería está integrada en el grupo atendido del Centro de Seguridad TIC AndalucíaCERT.

3. A los efectos de una mejor gestión de los incidentes, se actuará de forma coordinada con el Centro de Seguridad TIC AndalucíaCERT.

4. La Consejería tendrá un plan para mantener la continuidad TIC de los procesos y sistemas críticos y garantizar su recuperación en caso de un incidente que afecte gravemente a su disponibilidad. 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.

Artículo. 20. Formación y concienciación en seguridad TIC.

Periódicamente 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 la Consejería utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad TIC y de la normativa de seguridad TIC que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta, a través de cláusulas contractuales o acuerdos de nivel servicio, a las obligaciones generales establecidas en dicha normativa, pudiendo disponer la tercera parte de sus propios procedimientos operativos para satisfacerla. Se establecerán mecanismos de comunicación y resolución de incidencias. Se velará por que el personal de terceros esté adecuadamente concienciado en materia de seguridad, al menos, al mismo nivel que el establecido en esta política de seguridad TIC.

00182973

3. Cuando algún aspecto de esta política de seguridad TIC no pueda ser satisfecho por una tercera parte según se requiere en el párrafo anterior, se requerirá un informe de la Unidad de Seguridad TIC que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por las personas responsables de la información y/o los servicios afectados antes de proseguir en la relación con la tercera parte.

Artículo 22. Auditorías de la seguridad.

1. Los sistemas de información serán objeto de una auditoría regular ordinaria, al menos cada dos años, que verifique el cumplimiento de los requerimientos del ENS. Estas auditorías ordinarias así como las extraordinarias se harán de acuerdo con lo establecido en el art. 34 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica y la Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.

2. Los informes de auditoría serán presentados a la persona Responsable del Sistema competente, al Delegado o a la Delegada 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 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, en coordinación con la Unidad de Seguridad TIC Corporativa para aquellos agentes externos a la Junta de Andalucía, con otros agentes especializados en esta materia. En especial, se contemplarán los siguientes:

a) AndaluciaCERT.

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

c) Unidad de Seguridad TIC de la Junta de Andalucía.

d) Centro directivo con competencias en coordinación y seguimiento del cumplimiento de la normativa aplicable en materia de protección de datos.

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

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 Central de Investigación Tecnológica del Cuerpo Nacional de Policía, para la investigación de acciones relacionadas con la delincuencia informática y los fraudes en el sector de las telecomunicaciones.

00182973

CAPÍTULO III

Protección de datos de carácter personal

Artículo 24. Incidencia de la normativa de protección de datos de carácter personal.

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, a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y al 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.

Artículo 25. Responsables de los Tratamientos de datos de carácter personal.

1. Las personas 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, las personas Responsables de la Información, es decir, las personales titulares de los órganos directivos, tendrán la condición de Responsables del Tratamiento respecto a los tratamientos sobre los que determinen sus fines y medios, salvo que las normas aplicables sobre asignación de atribuciones en materia de protección de datos de carácter personal dispongan lo contrario.

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

Artículo 26. Encargados de los Tratamientos de datos de carácter personal.

1. Si las personas Responsables de los Tratamientos designaran a una persona Encargada del Tratamiento lo harán únicamente a una que ofrezca las garantías suficientes para aplicar las medidas técnicas y organizativas apropiadas para 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 la persona Responsable como la persona Encargada 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 una persona Encargada de Tratamiento sujeto a lo establecido en el artículo 28 de dicho Reglamento General de Protección de Datos.

Artículo 27. Delegado o Delegada de Protección de Datos.

1. En el ámbito de la Consejería se designará una persona que ostente la condición de Delegado o Delegada de Protección de Datos a efectos de lo establecido en los artículos 37 y 38 del Reglamento General de Protección de Datos. Las entidades dependientes de la Consejería como responsables de tratamiento de datos de carácter personal designarán en su ámbito un Delegado o Delegada de protección de datos.

00182973

2. La persona que ostente la condición de Delegado o Delegada de Protección de Datos será designada por la persona titular de la Viceconsejería entre personal funcionario adscrito a la Consejería, no pudiendo ser removida ni sancionada por desempeñar sus funciones, salvo que incurriera en dolo o negligencia grave en su ejercicio. La resolución por la que se 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 o Delegada 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 o Delegada 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 las personas Responsables de Tratamiento de la Consejería, debiendo éstos facilitarle la información necesaria para ello.

e) Asesorar a la persona 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 a la persona 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.

Disposición adicional primera. Constitución del Comité de Seguridad TIC.

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

Disposición adicional segunda. Actualización de la política de seguridad de la información.

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

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

Disposición derogatoria única. Derogación de normas.

Quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo establecido en la presente orden y, en particular, la Orden de 11 de febrero de 2008, por la que se crea el Comité de Seguridad y se aprueba el Documento de Política de Seguridad de la Información de la Consejería, publicada en el BOJA núm. 43 de 3 de Marzo de 2008.

00182973

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, 3 de diciembre de 2020

FRANCISCO JAVIER IMBRODA ORTIZ
Consejero de Educación y Deporte

00182973