3. Otras disposiciones

CONSEJO DE TRANSPARENCIA Y PROTECCIÓN DE DATOS DE ANDALUCÍA

Resolución de 12 de diciembre de 2019, de la Dirección del Consejo de Transparencia y Protección de Datos de Andalucía, por la que se establece la política de seguridad de las tecnologías de la información y de la comunicación del Consejo, así como la estructura organizativa responsable de su ejecución.

El artículo 43 de la Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía, crea el Consejo de Transparencia y Protección de Datos de Andalucía (en adelante, el Consejo), como autoridad independiente de control en materia de protección de datos y de transparencia en la Comunidad Autónoma de Andalucía, siendo una entidad pública con personalidad jurídica propia, con plena capacidad y autonomía orgánica y funcional para el ejercicio de sus cometidos.

Los avances tecnológicos en los ámbitos de la informática, de las telecomunicaciones y de la Sociedad de la Información son ya un hecho consolidado, que afecta no sólo a la sociedad sino también a los poderes públicos, siendo estos 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 las personas y a las empresas, como a las Administraciones Públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

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 configuran 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 aquéllas entre sí.

En concreto, la citada 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 de la comunicación (en adelante, TIC) de los últimos años y cómo este desarrollo afecta a las relaciones entre estos agentes, pretendiendo implantar una Administración totalmente electrónica, interconectada y transparente, mejorando la agilidad de los procedimientos administrativos y reduciendo los tiempos de tramitación.

Por otro lado, 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, Esquema Nacional de Seguridad), modificado por el Real Decreto 951/2015, de 23 de octubre, tiene por objeto regular el Esquema Nacional de Seguridad establecido en el artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos (derogada por la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas), y determinar la política de seguridad que se ha de aplicar en la utilización de los medios electrónicos a los que se refiere la citada Ley.

El Esquema Nacional de Seguridad está constituido por los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información. Será aplicado por las Administraciones Públicas para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias. De acuerdo con lo previsto en el artículo 11.1 del Esquema Nacional de Seguridad, todos los órganos superiores de las Administraciones Públicas deberán

00167026

disponer formalmente de su política de seguridad que articule la gestión continuada de la seguridad, que será aprobada por la persona titular del órgano superior correspondiente. Precisamente, en cumplimiento de esta previsión, se dicta la presente resolución.

Para el desarrollo de la presente política de seguridad TIC se ha tenido en cuenta el mencionado marco legal y regulatorio, así como lo dispuesto en el Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía, modificado por el Decreto 70/2017, de 6 de junio, así como la Resolución de 27 de septiembre de 2004, de la Secretaría General para la Administración Pública, por la que se establece el manual de comportamiento de los empleados públicos en el uso de los sistemas informáticos y redes de comunicaciones de la Administración de la Junta de Andalucía y 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.

Asimismo, en lo que se refiere al tratamiento de los datos personales resulta de aplicación 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, Reglamento General de Protección de Datos o RGPD), así como la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD).

En su virtud, en uso de las atribuciones que tengo conferidas por el artículo 10.3.b) del Decreto 434/2015, de 29 de septiembre, por el que se aprueban los Estatutos del Consejo de Transparencia y Protección de Datos de Andalucía,

D I S P O N G O

CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 1. Objeto.

La presente resolución tiene por objeto:

a) Definir la política de seguridad TIC del Consejo, conformando, junto a las disposiciones y documentos técnicos que la desarrollen, el marco regulador de la seguridad TIC.

b) Establecer la estructura organizativa responsable de su ejecución.

Artículo 2. Ámbito de aplicación

La presente política de seguridad TIC se aplicará a todos los activos de tecnologías de la información y de la comunicación del Consejo, y deberá ser observada por todo su personal, así como por cualquier otra persona que tenga acceso a cualquiera de dichos activos.

A estos efectos, se entenderá como un activo de tecnología de la información y de la comunicación cualquier información o sistema de información que tenga valor para el Consejo, incluyendo datos, servicios, aplicaciones, equipos, comunicaciones, instalaciones, procesos y recursos humanos.

Artículo 3. Definiciones, objetivos y principios.

La presente política de seguridad TIC del Consejo asume las definiciones, objetivos y principios establecidos en los artículos 2, 4 y 5 del Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información

00167026

y comunicaciones en la Administración de la Junta de Andalucía, modificado por el Decreto 70/2017, de 6 de junio.

CAPÍTULO II

ORGANIZACIÓN DE LA POLÍTICA DE SEGURIDAD TIC

Artículo 4. Estructura organizativa de la seguridad TIC.

1. La estructura organizativa de la gestión de la seguridad TIC estará integrada por las siguientes figuras:

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

2. Además, de acuerdo con lo exigido por la normativa sobre protección de datos personales, la presente política de seguridad contempla la participación de las siguientes figuras:

a) Responsable del tratamiento.
b) Delegado de Protección de Datos.
c) Encargado del tratamiento.

Artículo 5. Comité de Seguridad TIC.

1. Se crea el Comité de Seguridad TIC del Consejo como órgano no colegiado de dirección y seguimiento en materia de seguridad de los activos TIC de los que el Consejo sea titular o cuya gestión tenga encomendada.

2. El Comité de Seguridad TIC estará formado por los siguientes miembros:

a) Presidencia (con voz y voto): la persona titular de la Dirección del Consejo.
b) Vicepresidencia (con voz y voto): la persona titular de la Secretaría General.
c) Vocalías:
1º. La persona titular de la Dirección del Área de Transparencia (con voz y voto).
2º. La persona titular de la Dirección del Área de Protección de Datos (con voz y voto).
3.º Delegado de Protección de Datos (con voz y sin voto).
4.º Responsable de Seguridad TIC (con voz y sin voto).
d) Secretaría (con voz y voto): La persona titular del Servicio de Informática y Telecomunicaciones.

3. Cuando el tratamiento de determinadas cuestiones lo requiera, se podrá convocar a las reuniones del Comité de Seguridad TIC a personal técnico especializado, a los efectos de prestar asesoramiento experto.

4. El Comité de Seguridad TIC se reunirá, previa convocatoria, con carácter ordinario una vez al semestre y con carácter extraordinario por acuerdo de la presidencia, a iniciativa propia o previa solicitud razonada de uno de sus miembros. De sus reuniones se levantará acta.

5. En caso de necesidad, la Presidencia será suplida por la Vicepresidencia, y las personas titulares de la Vicepresidencia, Vocalías y Secretaría podrán proponer a la Presidencia su suplente entre el personal funcionario del Consejo.

6. Serán funciones propias del Comité de Seguridad TIC:

a) Definir, aprobar y realizar el 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) Nombrar a la persona Responsable de Seguridad TIC del Consejo.

d) Aprobar la normativa de seguridad TIC de segundo y tercer nivel del Consejo.

00167026

e) Establecer las directrices comunes y supervisar el cumplimiento de la normativa en materia de seguridad TIC.

f) Supervisar el nivel de riesgo y toma de decisiones en la respuesta a incidentes de seguridad TIC que afecten a los activos TIC.

g) Promocionar la formación, entrenamiento y concienciación sobre las medidas legales y organizativas relativas a la seguridad TIC entre el personal del Consejo.

h) Impulsar la determinación de los niveles de seguridad de la información tratada, en la que se valorarán los impactos que tendrán los incidentes que puedan afectar a la seguridad de la información.

i) Impulsar la realización de los preceptivos análisis de riesgos y establecer criterios para la aceptación, en su caso, de los riesgos residuales.

j) Proponer a la dirección del Consejo la actualización de la Política de Seguridad TIC a los efectos de adaptarla a nuevas circunstancias, técnicas u organizativas, para evitar su obsolescencia.

k) Determinar las actuaciones a realizar ante cualquier otra cuestión que pueda afectar a la seguridad de los activos.

Artículo 6. Responsable de la Información

1. Responsable de la Información será la persona titular de la dirección del Consejo, que es quien determina los requisitos de la información tratada en el mismo.

2. Sus funciones serán:

a) Determinar los niveles de seguridad de la información, de acuerdo con lo establecido en el Anexo I del Esquema Nacional de Seguridad.

b) Determinar los requisitos de seguridad TIC, categorizando la información mediante la valoración de los impactos de los incidentes que puedan producirse.

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

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

e) Determinar la suspensión del tratamiento de una cierta información o la prestación de un determinado servicio si se aprecian deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos, y tras tener en consideración la opinión de la persona Responsable del Servicio que pudiera estar afectado, de la persona Responsable de Seguridad TIC y del Delegado de Protección de Datos.

f) Desarrollar las funciones atribuidas a la figura del Responsable de la Información derivadas de la aplicación del Esquema Nacional de Seguridad o de cualquier otra normativa de seguridad que pudiera afectarle.

3. El nombramiento, renovación o cese de la persona que desempeñe las funciones de Responsable de la Información, está aparejado de forma automática a su toma de posesión, renovación o cese en la titularidad en la dirección del Consejo.

Artículo 7. Responsable de Seguridad TIC.

1. El Consejo dispondrá de una persona como Responsable de Seguridad TIC que será nombrada o cesada por decisión del Comité de Seguridad TIC, notificándose dicha decisión a la persona correspondiente.

2. La persona Responsable de Seguridad TIC tendrá las siguientes funciones:

a) Determinar las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

b) Desarrollar labores de soporte, asesoramiento e información al Comité de Seguridad TIC, así como de ejecución de las decisiones y acuerdos adoptados por este.

00167026

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

d) Definir, implantar y mantener los controles de carácter organizativo para la protección de los datos, aplicaciones y sistemas, así como coordinar la realización y mantenimiento de los análisis de riesgos del Consejo.

e) Supervisar sistemáticamente los controles de carácter procedimental, operacional y medidas técnicas de protección de los datos, aplicaciones y sistemas del Consejo.

f) Definir y supervisar los criterios y requisitos técnicos de seguridad aplicados en las distintas fases del ciclo de vida de los soportes, sistemas y aplicaciones del Consejo. Antes de la puesta en producción de nuevos sistemas de información o de evolutivos de los existentes, evaluar los aspectos de seguridad y comunicar los posibles riesgos al centro o centros directivos responsables de la información y del servicio.

g) Definir y ejecutar los programas formativos y de concienciación relacionados con buenas prácticas de seguridad TIC en el ámbito del Consejo.

h) Organizar, actualizar y custodiar la documentación de seguridad, así como gestionar los mecanismos de acceso a la misma.

i) Informar al Comité de Seguridad TIC, en cada una de sus reuniones, de aquellas incidencias o deficiencias que pudieran haberse producido en materia de seguridad, de modo que el Comité de Seguridad TIC disponga de información completa y pueda arbitrar los mecanismos necesarios para su subsanación.

j) Desarrollar cuantas otras funciones le sean encomendadas por el Comité de Seguridad TIC del Consejo, así como las que se deriven de la aplicación del Esquema Nacional de Seguridad.

3. La persona Responsable de Seguridad TIC 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 Responsable de la Información, Responsable del Servicio y Responsable del Sistema. Dicho inventario se mantendrá permanentemente actualizado y a disposición del Comité de Seguridad TIC.

Artículo 8. Responsable del Servicio.

1. Tendrán la consideración de Responsable del Servicio las personas titulares de la Secretaría General del Consejo, del Área de Transparencia y del Área de Protección de Datos, quienes determinan los requisitos de los servicios prestados en el ámbito de sus competencias.

2. El nombramiento por parte de la dirección del Consejo de las personas titulares de la Secretaría General y cada una de las Áreas supondrá, con carácter nato, asumir las funciones de Responsable del Servicio en relación con su ámbito competencial.

3. Las principales funciones de la persona Responsable del Servicio, dentro de su ámbito de competencia, son las siguientes:

a) Colaborar en la determinación de los requisitos de seguridad de los servicios a prestar, categorizando los servicios mediante la valoración de los impactos de los incidentes que puedan producirse.

b) Proporcionar la información necesaria a la persona Responsable de Seguridad TIC para realizar los preceptivos análisis de riesgos, con la finalidad de establecer las salvaguardas a implantar.

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

Artículo 9. Responsable del Sistema.

1. Cada uno de los sistemas de información del Consejo dispondrá de una persona Responsable del Sistema, correspondiendo su designación, previa consulta con el correspondiente Responsable del Servicio, a la persona titular del Servicio de Informática

00167026

y Telecomunicaciones entre las personas pertenecientes a dicho servicio o a las entidades que, a través del contrato o vínculo jurídico correspondiente, den soporte externo a los sistemas de información. Una misma persona podría ser Responsable de varios sistemas de información.

2. Las funciones de las personas Responsables de los Sistemas serán:

a) Coordinar el desarrollo, operación y mantenimiento del sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones técnicas, instalación y verificación de su correcto funcionamiento.

b) Definir la tipología y la gestión del sistema de información, estableciendo los criterios de uso y los servicios disponibles en el mismo.

c) Verificar que las medidas de seguridad que deban ser aplicadas se integren adecuadamente en el marco general de seguridad.

d) Asumir la responsabilidad directa de la seguridad de los sistemas de información que estén a su cargo, 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 persona Responsable de Seguridad TIC del Consejo.

e) Crear, mantener y actualizar de forma permanente la documentación de seguridad de los sistemas de información, con el asesoramiento de la persona Responsable de Seguridad TIC.

f) Aprobar toda modificación sustancial de la configuración de cualquier elemento técnico que dé soporte al sistema de información.

g) Colaborar en el proceso de la gestión y análisis de riesgos.

h) Proponer a la persona Responsable de la Información, a través de la persona Responsable de Seguridad TIC, la suspensión del tratamiento de una cierta información o la prestación de un determinado servicio si aprecia deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos.

Artículo 10. Resolución de conflictos.

Los conflictos o discrepancias entre los diferentes responsables serán resueltos por la dirección del Consejo, oído el Comité de Seguridad TIC del Consejo. Dicho Comité podrá proponer a la dirección del Consejo el establecimiento de un procedimiento específico para la resolución de conflictos.

CAPÍTULO III

GESTIÓN DE LA POLÍTICA DE SEGURIDAD TIC

Artículo 11. Gestión de riesgos.

1. La gestión de riesgos comprenderá tanto los riesgos relativos a la seguridad de los sistemas de información como los relativos a la protección de datos personales. Para cada tipo de riesgos se utilizarán las metodologías de análisis y gestión de riesgos que resulten más adecuadas.

2. La gestión de riesgos debe realizarse de manera continua, conforme a los principios de gestión de la seguridad basada en los riesgos y reevaluación periódica.

3. El Responsable de la Información y el Responsable del Servicio son responsables de la gestión de los riesgos en su ámbito de competencia y, en consecuencia, de aceptar los riesgos residuales calculados en el análisis de riesgos, así como de realizar su seguimiento y control.

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

00167026

5. La selección de las medidas de seguridad a aplicar será propuesta por la persona Responsable de Seguridad TIC al Comité de Seguridad TIC. Corresponderá a aquella el seguimiento de su aplicación, una vez adoptadas.

6. Anualmente se revisará por la persona Responsable de Seguridad TIC el proceso de gestión de riesgos en todas sus fases, elevando el correspondiente informe al Comité de Seguridad TIC.

Artículo 12. Gestión de incidentes de seguridad y de la continuidad.

1. Para la gestión de incidentes de seguridad, que incluye la prevención, detección, reacción y recuperación, se estará a lo dispuesto en la normativa reguladora de Esquema Nacional de Seguridad, así como 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 con el fin de 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. Para gestionar adecuadamente los posibles incidentes de seguridad se actuará de forma coordinada con AndalucíaCERT.

4. En caso de violaciones de seguridad de los datos personales el Consejo actuará de acuerdo con lo dispuesto en el Reglamento General de Protección de Datos.

Artículo 13. Desarrollo normativo de la política de seguridad TIC.

1. El conjunto de normas sobre seguridad TIC del Consejo es de obligado cumplimiento y se desarrollará en tres niveles, según el ámbito de aplicación y nivel de detalle técnico, de manera que cada norma de un determinado nivel de desarrollo se fundamente en las normas de nivel superior. Dichos niveles de desarrollo normativo son los siguientes:

a) Primer nivel normativo: Política de seguridad TIC, constituida por el presente documento.

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, y que deberán ser aprobadas por el Comité de Seguridad TIC, a propuesta de la persona Responsable de Seguridad TIC.

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. Estas normas serán aprobadas por el Comité de Seguridad TIC, a propuesta de la Secretaría General.

2. Además de los documentos citados en el apartado anterior, la documentación de seguridad TIC del Consejo podrá contar con otros documentos de carácter no normativo como pueden ser: recomendaciones, buenas prácticas, informes, registros, evidencias electrónicas, etc.

3. El Comité de Seguridad TIC establecerá los criterios necesarios para publicar y compartir la documentación derivada del desarrollo normativo de la política de seguridad TIC. La persona Responsable de Seguridad TIC, deberá mantener la documentación de seguridad actualizada y organizada, así como gestionar los mecanismos de acceso a la misma.

Artículo 14. Obligaciones del personal.

1. El personal que preste servicios en el Consejo, así como las personas que formen parte de su Comisión Consultiva, tiene la obligación de conocer y cumplir la política de seguridad TIC y la normativa de seguridad derivada en relación con el ejercicio de sus

00167026

funciones, siendo responsabilidad del Comité de Seguridad TIC disponer los medios necesarios para que la información llegue a las personas afectadas.

2. El personal que se incorpore al Consejo o que tenga acceso a alguno de sus sistemas de información o a la información gestionada por ellos deberá ser informado de la política de seguridad TIC y de la normativa de protección de datos que pudieran afectarle.

3. Procederá el ejercicio de las acciones pertinentes para la exigencia de las responsabilidades legales que correspondan por el incumplimiento de la política de seguridad TIC, de la normativa de seguridad derivada y de la normativa de protección de datos.

4. El personal del Consejo está sujeto a las instrucciones y normas que regulen el comportamiento del empleado público en el uso de los sistemas informáticos y redes de comunicaciones de la Administración de la Junta de Andalucía, así como a las que corresponden a la normativa de protección de datos personales.

Artículo 15. Formación y concienciación en privacidad y seguridad.

El Consejo desarrollará actividades de formación y concienciación en privacidad y seguridad TIC destinadas a su personal. Entre tales actividades se incluirán las de difusión de esta política de seguridad TIC y de las normas que la desarrollen.

Artículo 16. Otras personas o entidades.

1. Cualquier otra persona o entidad, externas al Consejo, que preste servicios al mismo deberá cumplir con la presente política de seguridad TIC en el grado que afecte al servicio que presten, debiendo ser informadas de dicha política y estableciéndose el compromiso de su cumplimiento a través de cláusulas contractuales, acuerdos de nivel de servicio o el vínculo jurídico que regule la correspondiente relación, debiéndose constituir los mecanismos adecuados para la comunicación y resolución de incidencias.

2. Cuando algún aspecto de esta política de seguridad TIC pudiera, debido a una circunstancia excepcional no prevista, no ser satisfecho por el prestador del servicio, según lo expresado en el párrafo anterior, se requerirá un informe de la persona Responsable de Seguridad TIC que precise los riesgos en que se incurre y la forma de tratarlos para comenzar o dar continuidad al servicio afectado. Para ello, se requerirá la aprobación de este informe por la persona Responsable de la Información, recabada la opinión de la persona Responsable del Servicio afectado.

Artículo 17. Auditorías de seguridad.

1. El Consejo auditará sus sistemas de información de forma periódica con objeto de revisar el cumplimiento de la normativa vigente en materia de seguridad TIC.

2. Los sistemas de información del Consejo serán objeto, al menos cada dos años, de una auditoría regular ordinaria que verifique el cumplimiento de los requisitos exigidos por el Esquema Nacional de Seguridad y de cualquier otra norma que requiera la realización de auditorías periódicas. La persona Responsable de Seguridad TIC coordinará el desarrollo y ejecución de las 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. En el caso de sistemas de información de categoría 'básica', según los términos del Esquema Nacional de Seguridad, esta auditoría podrá ser sustituida por una autoevaluación, de acuerdo con lo establecido en el mismo.

5. Los informes de auditoría serán presentados a las personas Responsables de los Servicios, Responsable de Seguridad TIC y Responsables de los Sistemas, y un resumen ejecutivo del mismo se facilitará a la dirección del Consejo y al Comité de Seguridad TIC.

6. La persona responsable de Seguridad TIC propondrá al Comité de Seguridad TIC, con base en el informe de auditoría, las medidas correctoras que deban abordarse

00167026

cuya aprobación dependa del mencionado Comité y coordinará la puesta en marcha de aquellas que sean aprobadas.

Gestionará igualmente la implantación de medidas cuya aprobación no dependa del Comité de Seguridad TIC, en coordinación con las personas Responsables de los Servicios afectados.

Artículo 18. 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, se fomentará el establecimiento de mecanismos de comunicación con otros agentes especializados en esta materia. En especial, se contemplarán los siguientes:

- Comité de Seguridad TIC de la Junta de Andalucía.
- Unidad de Seguridad TIC Corporativa de Andalucía.
- AndalucíaCERT: Centro experto para la prevención, detección y respuesta a incidentes y amenazas de seguridad en el ámbito de la Administración de la Junta de Andalucía.
- CCN-CERT: Centro Criptológico Nacional, como soporte y coordinación para la resolución de incidentes que sufra la Administración General, Autonómica o Local.
- AEPD: Agencia Española de Protección de Datos, así como otras autoridades de control en materia de protección de datos personales.
- INCIBE: Instituto Nacional de Ciberseguridad.
- BIT: 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.

Artículo 19. Actualización permanente y revisiones periódicas.

1. Esta resolución 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 20. Difusión de la política de seguridad TIC.

A los efectos de su difusión entre el personal del Consejo y de otras partes interesadas, la presente resolución se publicará en el Boletín Oficial de la Junta de Andalucía, y se difundirá a través de los medios que se establezcan por el Comité de Seguridad TIC.

CAPÍTULO IV

SOBRE PROTECCIÓN DE DATOS PERSONALES

Artículo 21. Incidencia de la normativa de protección de datos personales.

1. Para el desarrollo de la política de seguridad TIC del Consejo se seguirá en todo momento lo establecido en el Reglamento General de Protección de Datos, en la LOPDGDD y en la legislación nacional y autonómica vigente en cada momento en relación con esta materia.

2. Para todos los tratamientos de datos personales del Consejo, automatizados o no, deberán establecerse las medidas técnicas y organizativas apropiadas para garantizar una seguridad adecuada de los citados datos, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental.

00167026

3. El establecimiento de las mencionadas medidas se realizará teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines de los tratamientos de datos personales, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas. En caso de posible conflicto entre las medidas derivadas de la protección de datos personales y otras que se deriven del desarrollo de la presente política de seguridad TIC, prevalecerá el criterio que presente un mayor nivel de exigencia respecto a la protección de los datos personales.

Artículo 22. Responsable del tratamiento.

El Consejo será el Responsable del tratamiento de datos personales, en los términos del artículo 4.7 del Reglamento General de Protección de Datos.

Artículo 23. Delegado de Protección de Datos.

1. El Consejo dispondrá de un grupo de personas, denominado Grupo Delegado de Protección de Datos, que ostente la condición de Delegado de Protección de Datos a los efectos de lo establecido en los artículos 37 al 39 del Reglamento General de Protección de Datos y en el Capítulo III de la LOPDGDD.

2. El Grupo Delegado de Protección de Datos constará de un mínimo de dos personas y un máximo de cuatro, entre el personal que forme parte de la plantilla del Consejo.

3. La designación de cada una de las personas que formen parte del Grupo Delegado de Protección de Datos se realizará y comunicará, mediante acto documentado, por decisión de la dirección del Consejo y cada una de ellas será designada atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39 RGPD.

Las personas que formen parte del Grupo Delegado de Protección de Datos podrán desempeñar otras funciones y cometidos dentro del Consejo, siempre que dichas funciones y cometidos no den lugar a conflicto de intereses.

4. El cese de funciones de una persona como miembro del Grupo Delegado de Protección de Datos se realizará y comunicará, mediante acto motivado, por decisión de la dirección del Consejo.

5. La dirección del Consejo designará, entre las que formen parte del Grupo Delegado de Protección de Datos, a una persona que ostente la representación de dicho grupo, y que participará en las reuniones del Comité de Seguridad TIC.

Artículo 24. Encargados del tratamiento.

1. De conformidad con el artículo 4.8 RGPD será Encargado del tratamiento la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del Responsable del tratamiento.

2. La Dirección del Consejo velará para que la elección de los Encargados del tratamiento ofrezca las garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos exigidos por el Reglamento General de Protección de Datos y garantice la protección de los derechos de los interesados, conforme establece el artículo 28.1 del citado Reglamento.

3. Cuando el Encargado del tratamiento preste su servicio en régimen de concesión, encomienda de gestión, contrato o cualquier otro vínculo jurídico, las medidas de seguridad a aplicar sobre los tratamientos de datos personales se corresponderán con las establecidas por el Consejo y se ajustarán al Esquema Nacional de Seguridad.

4. El contrato o acto jurídico que vincule al Consejo y al Encargado del tratamiento deberá atender a las condiciones establecidas en el artículo 28 RGPD y demás normativa de aplicación.

00167026

5. El Encargado del tratamiento será informado por el Consejo de los requisitos exigidos, en función del servicio que vaya a prestar, por su política de seguridad TIC, siéndole de aplicación lo expresado en el artículo 16.

Disposición adicional única. Constitución del Comité de Seguridad TIC.

La primera reunión del Comité de Seguridad TIC tras la entrada en vigor de la presente política de seguridad TIC tendrá por objeto la constitución, renovación o confirmación del mismo y se celebrará en un plazo máximo de un mes a partir de la entrada en vigor de la presente resolución.

Disposición final. Entrada en vigor.

La presente resolución entrará en vigor el día siguiente al de su publicación en el Boletín Oficial de la Junta de Andalucía.

Sevilla, 12 de diciembre de 2019.- El Director, Manuel Medina Guerrero.

00167026