RESOLUCIÓN DE 26 DE JULIO DE 2024 DEL DEFENSOR DEL PUEBLO ANDALUZ Y DE LA INFANCIA Y ADOLESCENCIA DE ANDALUCÍA POR LA QUE SE APRUEBAN LAS NORMAS QUE REGULAN LA POLÍTICA DE SEGURIDAD DE INFORMACIÓN DE LA INSTITUCIÓN.

La Disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos de Carácter Personal y Garantía de Derechos Digitales prevé, en su apartado segundo, que los responsables enumerados en el artículo 77.1 de dicha ley orgánica deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad.

Asimismo, en virtud de dicho precepto, en los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad.

Por su parte, el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, requiere la tenencia de una política de seguridad aprobada por el órgano competente. De este modo, la presente Política de Seguridad de la Información viene a dar cumplimiento a las exigencias previstas en el ordenamiento, conteniendo directrices que rigen la forma en que la Institución del Defensor del Pueblo Andaluz y de la Infancia y Adolescencia de Andalucía gestiona y protege la información que trata y los servicios que presta.

Para su elaboración se han tenido en cuenta, además de la normativa ya citada, las recomendaciones y guías CCN-STIC del Centro Criptológico Nacional, particularmente de la serie 800, relacionadas con el Esquema Nacional de Seguridad.

Por lo expuesto, el Defensor del Pueblo Andaluz y de la Infancia y Adolescencia de Andalucía, en el ejercicio legítimo de sus competencias, establecidas en la Ley 9/1983, de 1 de diciembre, y en el artículo 11 de su Reglamento de Organización y Funcionamiento,

RESUELVE:

Primero.- Aprobar las normas que regulan la política de seguridad de información del Defensor del Pueblo Andaluz y de la Infancia y Adolescencia de Andalucía.

Segundo.- Ordenar su publicación en el Portal de Transparencia del Defensor del Pueblo Andaluz de conformidad con lo dispuesto en el artículo 6.1 de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno y en el artículo 10 de la Ley 1/2014, de 24 de junio, de transparencia pública de Andalucía.

El Defensor del Pueblo Andaluz.

Firmado por MAEZTU GREGORIO DE TEJADA JESUS - ***5028** el día 26/07/2024 con un certificado

Don Jesús Maeztu Gregorio de Tejada.

NORMAS QUE REGULAN LA POLÍTICA DE SEGURIDAD DE INFORMACIÓN DEL DEFENSOR DEL PUEBLO ANDALUZ Y DE LA INFANCIA Y ADOLESCENCIA DE ANDALUCÍA.

Artículo 1. Misión estatutaria y objeto del presente acuerdo.

1. El Defensor del Pueblo Andaluz y de la Infancia y Adolescencia de Andalucía es el Comisionado del Parlamento de Andalucía al que, atendiendo a las competencias que la Constitución atribuye al Defensor del Pueblo en su artículo 54 y la Ley Orgánica 2/2007, de 19 de marzo, de reforma del Estatuto de Autonomía para Andalucía, corresponde la defensa de los derechos y libertades comprendidos en el título primero de la Constitución, así como de los menores de edad según lo dispuesto en el artículo 24 de la Ley 4/2021, de 27 de julio, de Infancia y Adolescencia de Andalucía.

2. Es objeto de la presente Resolución aprobar la Política de Seguridad de la Información (en adelante PSI) del Defensor del Pueblo Andaluz y de la Infancia y Adolescencia de Andalucía, así como la estructura organizativa necesaria para definirla, implantarla y gestionarla.

Artículo 2. Ámbito de aplicación.

1. La PSI en el Defensor del Pueblo Andaluz y de la Infancia y Adolescencia de Andalucía afectará a la información tratada por medios electrónicos y a la información en soporte no electrónico que haya sido causa o consecuencia directa de la información electrónica, gestionada por la Institución en el ámbito de sus competencias.

2. La PSI y su normativa de desarrollo será de obligado cumplimiento para todo el personal que acceda tanto a los sistemas de información como a la propia información que sea gestionada por la Defensoría, con independencia de cuál sea su destino, adscripción o relación con la misma.

Artículo 3. Marco normativo.

Las disposiciones normativas que resultan de aplicación vienen determinadas por el artículo 54 de la Constitución Española, la Ley Orgánica 2/2007, de 19 de marzo, de reforma del Estatuto de Autonomía para Andalucía en su artículo 128 en relación con la Ley 9/1983, de 1 de diciembre, del Defensor del Pueblo Andaluz, el conjunto de normas y Resoluciones dictadas por el titular de la Institución que la regula, así como 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 la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos de Carácter Personal y Garantía de Derechos Digitales.

Artículo 4. Objetivos y principios de la seguridad de la información.

Los principios básicos son directrices fundamentales de seguridad que han de tenerse siempre presentes en cualquier actividad relacionada con el uso de los activos de

información.

Se establecen los siguientes:

- Seguridad como proceso integral.
- Gestión de la seguridad basada en los riesgos.
- Prevención, detección, respuesta y conservación.
- Existencia de líneas de defensa.
- Vigilancia continua.
- Reevaluación periódica.
- Diferenciación de responsabilidades.

Y por ello, se desarrollará aplicando los siguientes requisitos mínimos:

- Organización e implantación del proceso de seguridad.
- Análisis y gestión de los riesgos.
- Gestión de personal.
- Profesionalidad.
- Autorización y control de los accesos.
- Protección de las instalaciones.
- Adquisición de productos de seguridad y contratación de servicios seguridad.
- Mínimo privilegio.
- Integridad y actualización del sistema.
- Protección de la información almacenada y en tránsito.
- Prevención ante otros sistemas de información interconectados.
- Registros de la actividad y detección de código dañino.
- Incidentes de seguridad.
- Continuidad de la actividad.
- Mejora continua del proceso de seguridad.

En cuanto a los objetivos de la Seguridad de la información en el Defensor del Pueblo Andaluz y de la Defensoría de la Infancia y Adolescencia en Andalucía, se fijan los siguientes:

- Garantizar la calidad y protección de la información.

- Lograr la plena concienciación de las personas usuarias respecto a la seguridad de la información.

- Gestión de activos de información: Los activos de información del dPA se encontrarán inventariados y categorizados y estarán asociados a un responsable.

- Seguridad ligada a las personas: Se implantarán los mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un su uso indebido, logrando la plena concienciación de las personas usuarias respecto a la seguridad de la información.

- Seguridad física: Los activos de información serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.

- Seguridad en la gestión de comunicaciones y operaciones: Se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las TIC. La información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.

- Control de acceso: Se limitará el acceso a los activos de información por parte de las personas usuarias, procesos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo. Además, quedará registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso y auditar su uso adecuado, conforme a la actividad de la organización.

- Adquisición, desarrollo y mantenimiento de los sistemas de información: Se contemplarán los aspectos de seguridad de la información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.

- Gestión de los incidentes de seguridad: Se implantarán los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.

- Garantizar la prestación continuada de los servicios: Se implantarán los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de sus procesos de negocio, de acuerdo con

las necesidades de nivel de servicio de sus usuarios.

- Protección de datos: Se adoptarán las medidas técnicas y organizativas que corresponda implantar para atender los riesgos generados por el tratamiento para cumplir la legislación de seguridad y privacidad.

- Cumplimiento: Se adoptarán las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información.

Artículo 5. Estructura organizativa.

La estructura organizativa para la gestión de la seguridad de la información en la Defensoría, de acuerdo con el principio de función diferenciada, estará compuesta por los siguientes agentes:

a) Comité de Dirección de Seguridad de la Información.

b) Responsable de Seguridad.

c) Responsable del Sistema de Información.

d) Responsable de la Información.

e) Delegado/a de Protección de Datos.

f) Responsables de los Servicios.

Artículo 6. Comité de Dirección de Seguridad de la Información.

1. Se crea, adscrito a la persona titular del cargo de Defensor del Pueblo Andaluz, el Comité de Dirección de Seguridad de la Información (en adelante, CDSI), que gestionará y coordinará todas las actividades relacionadas con la seguridad de los sistemas de información.

2. El CDSI estará compuesto por los siguientes miembros:

a) Presidencia: La persona titular de la Institución.

b) Vocalías:

- La persona titular de la Secretaría General de la Institución.

- Una persona titular de una Adjuntía.

- Responsable del sistema de información.

- Responsables de la información y de los servicios.

- Delegado/a de protección de datos, con voz y sin voto.

- Un/a responsable de los Servicios, designado con carácter rotatorio y periodicidad anual.

c) Secretaría: Responsable de seguridad.

3. El régimen de suplencia de la persona titular, secretaría y vocalías, en caso de vacante, ausencia o enfermedad, así como en los casos en que haya sido declarada su abstención o recusación y, en general, cuando concurra alguna causa justificada, se establece del siguiente modo:

- La persona titular de la Presidencia será sustituida por la adjuntía que hubiese sido designada para ocupar la vocalía del CDSI.

- Los demás miembros del CDSI serán sustituidos por las personas que designe quien ostente la Presidencia.

4. Tendrán la consideración de miembros permanentes:

- La persona titular de la Institución.

- La persona titular de la Secretaría General de la Institución, que será responsable de información.

- La Adjuntía que hubiese sido designada como vocal.

- La persona responsable del sistema de información.

- La persona responsable de seguridad.

- El/La Delegado/a de protección de datos.

- La persona designada entre los Responsables de los Servicios.

5. Tendrán la consideración de miembros no permanentes las personas responsables de los servicios, departamentos y unidades que sean convocados/as por la presidencia en función de los asuntos a tratar, en representación de los distintos ámbitos o áreas de seguridad TIC del dPA.

Adicionalmente, y con la condición de miembros no permanentes, la presidencia del CDSI podrá invitar a personas responsables de materias específicas a tratar, en función del contenido del orden del día.

En todo caso, los miembros no permanentes tendrán voz pero no tendrán voto.

6. El CDSI ejercerá las siguientes funciones:

a) Impulsar el desarrollo normativo de la PSI y velar por el cumplimiento de la misma y demás normativa de seguridad aprobada.

b) Promover revisiones y actualizaciones de la PSI y de su normativa de desarrollo.

c) Proporcionar soporte, asesoramiento e información a la alta dirección, así como ejecutar los acuerdos adoptados por éste en materia de seguridad de la información.

d) Aprobación de guías de seguridad a propuesta del Responsable de Seguridad.

e) Resolver los conflictos que puedan surgir entre los diferentes agentes participantes en la gestión de la seguridad de la información.

f) Ordenar la realización de las auditorías o autoevaluaciones de seguridad y recibir información de los resultados de las mismas. En este sentido, también podrá definir la planificación de estas actuaciones, que en todo caso deberán ser regulares.

g) Aprobar los planes de mejora de la seguridad en su ámbito de competencias.

h) Tomar conocimiento de las decisiones y medidas tomadas para satisfacer los requisitos de seguridad de la información y de los servicios.

i) Establecer los requisitos de seguridad que deben cumplir, a nivel organizativo, técnicos y de control, los sistemas y servicios de la Defensoría.

j) Tomar conocimiento de los incidentes de seguridad que se produzcan.

k) Promover la formación y concienciación en materia de seguridad de la información a todo el personal, definiendo los programas formativos y de concienciación relacionados con buenas prácticas de seguridad TIC en el ámbito del Defensor del Pueblo Andaluz.

l) Aprobación y revisión anual del Proceso de Gestión de Riesgos especificado en el artículo 13.

7. Las sesiones del CDSI se considerarán debidamente constituidas cuando asistan a sus reuniones al menos la persona titular de la presidencia y el/la secretario/a del CDSI, o personas que las sustituyan, y otros/as dos vocales.

8. El CDSI se reunirá con carácter ordinario al menos una vez al año, y con carácter extraordinario cuando lo decida la persona titular de la Presidencia, de oficio o a propuesta de alguno de sus miembros, y siempre que se produzca alguno de los siguientes supuestos:

a) Se produzcan incidencias de seguridad graves que afecten a cualquier sistema o a la seguridad interior

b) Surjan nuevas necesidades de seguridad que requieran la participación del Comité.

9. El CDSI se regirá por las normas de funcionamiento previstas en la presente Resolución.

Artículo 7. Oficina de seguridad TIC

1. En el contexto de gobernanza de la ciberseguridad de la Institución se podrá constituir la Oficina de Seguridad TIC.

2. Se compone de los siguientes miembros, con carácter permanente:

- Responsable de Seguridad
- Responsable del Sistema de información.
- Persona titular de la Secretaría General, como responsable de información.
- Asesor/a técnico de la Secretaría General.

Podrán ser convocadas, como miembros no permanentes, personas expertas y especialistas de seguridad (interno o externo al dPA) que el Responsable de Seguridad considere de utilidad.

3. Serán funciones de la Oficina de Seguridad TIC:

a) Las labores de soporte, asesoramiento e información al CDSI, así como de ejecución de las decisiones y acuerdos adoptados por éste.

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

c) La 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. Estas funciones se desempeñarán con el asesoramiento del delegado de protección de datos.

d) La supervisión sistemática de los controles de carácter procedimental, operacional y de las medidas técnicas de protección de los datos, las aplicaciones y los sistemas.

e) La 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 por parte de las unidades responsables de la prestación de los servicios TIC, para lo que deberá contar con el asesoramiento del delegado de protección de datos.

f) Antes de la puesta en producción de nuevos sistemas de información o de la evolución de los existentes, la Unidad de Seguridad TIC deberá evaluar los aspectos de seguridad y comunicar los posibles riesgos al responsable de la información y de los servicios.

g) La definición y ejecución de los programas formativos y de concienciación relacionados con las buenas prácticas de seguridad TIC.

h) La elaboración y mantenimiento de un inventario de servicios y sistemas, con indicación expresa, para cada uno de ellos, de las figuras de responsable de la información, responsable del servicio, responsable del sistema y responsable de seguridad TIC.

4. La persona responsable de la Unidad de Seguridad TIC de la Institución tendrá la condición de responsable de seguridad TIC del mismo.

5. La persona responsable de la seguridad TIC y aquellas otras que, en su caso, compongan la Unidad de Seguridad TIC podrán formar parte de la plantilla del Defensor del Pueblo de Andalucía o desempeñar sus funciones en el marco de un contrato de servicios, convenio o cualquier otro instrumento jurídico que haga posible dicha participación.

6 La designación de la persona responsable de la seguridad TIC y de aquellas otras que, en su caso, compongan la Unidad de Seguridad TIC se llevará a cabo por parte del CDSI de la Institución.

7. Se reunirá, al menos, una vez al trimestre y siempre antes de la celebración de las reuniones del CDSI.

Artículo 8. Responsable de Seguridad.

1. La persona Responsable de la Seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones.

2. Serán funciones de la persona Responsable de Seguridad, las señaladas para la Oficina de Seguridad TIC cuando ésta no hubiese sido constituida, y adicionalmente las siguientes:

a) Mantener y verificar el nivel adecuado de seguridad de la Información manejada y de los Servicios electrónicos prestados por los sistemas de información.

b) Promover la formación y concienciación en materia de seguridad de la información.

c) Designar responsables de la ejecución del análisis de riesgos, de la Declaración de Aplicabilidad, identificar medidas de seguridad, determinar configuraciones necesarias, colaborar y asesorar en la elaboración de documentación del sistema.

d) Proporcionar asesoramiento para la determinación de la Categoría del Sistema, en colaboración con el Responsable del Sistema y/o Comité de Seguridad TIC.

e) Participar en la elaboración e implantación de los planes de mejora de la seguridad y, llegado el caso, en los planes de continuidad, procediendo a su validación.

f) Gestionar las revisiones externas o internas del sistema.

g) Gestionar los procesos de certificación.

h) Elevar al Comité de Seguridad la aprobación de cambios y otros requisitos del sistema.

i) Aprobar los procedimientos de seguridad que forman parte del Mapa Normativo (y no son competencia del Comité) y poner en conocimiento al Comité de las modificaciones que se hayan realizado a lo largo del periodo en curso.

j) Monitorización de los incidentes de seguridad y supervisar su investigación.

k) Habilitar y mantener un registro de incidencias para la seguridad de la información
que esté bajo su responsabilidad. Este registro deberá estar disponible para cualquier revisión o auditoría.

l) Mantener un listado actualizado del personal autorizado a acceder a los sistemas
de información.

m) Revisar los permisos y perfiles de acceso de la información que se encuentran bajo su gestión.

n) Constituirse como punto de contacto para la coordinación con el CERT de referencia y con la autoridad competente en materia de seguridad de las redes y sistemas de información.

o) Notificar a la autoridad competente, a través del CERT de referencia y sin dilación indebida, los incidentes que tengan efectos perturbadores en la prestación de los servicios.

3. En su condición de Secretario/a del CDSI, la persona Responsable de Seguridad tiene como funciones:

a) Trasladar a los miembros del CSDI la convocatoria de las reuniones de dicho órgano.

b) Preparar los temas a tratar en las reuniones del CDSI, aportando información puntual para la toma de decisiones, preparando todos los trabajos previos necesarios para las reuniones, apoyándose cuando lo requiera en las distintas áreas, servicios o unidades del Defensor del Pueblo Andaluz.

c) Elaborar y custodiar las actas de las reuniones.

d) Velar por la ejecución de las decisiones del CDSI.

4. El rol de Responsable de Seguridad será desempeñado por la persona que designe el titular de la Defensoría, que en todo caso será distinto de la persona Responsable del Sistema de Información. Reportará directamente a la persona titular del cargo del Defensor del Pueblo Andaluz, a la persona titular de la Secretaría General y al CDSI en relación con sus funciones como Responsable de Seguridad.

Artículo 9. Responsable del Sistema de Información.

1. La persona Responsable del Sistema de Información se encargará de la implementación de la seguridad en el sistema y de la supervisión de la operación diaria del mismo.

2. Dentro de sus funciones se encuentran las siguientes:

a) Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento

b) Definir la topología y sistemas de gestión de los sistemas de información, estableciendo los criterios de uso y los servicios disponibles en éstos.

c) Cerciorarse de que las medidas de seguridad se integran adecuadamente dentro del marco tecnológico y de seguridad de la Institución.

d) Adoptar las medidas correctoras adecuadas de acuerdo con las evaluaciones y auditorías de seguridad.

e) Responsabilizarse del desarrollo, operación y mantenimiento de los sistemas de información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.

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

g) Colaborar con el Responsable de Seguridad en la elaboración de procedimientos de seguridad de los sistemas de información.

h) Elaborar planes de continuidad de los sistemas de información.

i) Acordar la suspensión del manejo de determinada 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 deberá ser acordada con la persona Responsable de la Información, la persona Responsable del Servicio/s afectada/s, y la persona Responsable de Seguridad antes de ser ejecutada, e informado el CDSI.

j) La gestión de las autorizaciones concedidas a las personas usuarias del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado.

k) Autorizar los permisos de acceso a los usuarios sobre los recursos, (automatizados y no automatizados) que se encuentran bajo su responsabilidad y que sean estrictamente necesarios para el desarrollo de las funciones de/l/la trabajador/a.

3. El rol de Responsable del Sistema de Información recaerá en la persona titular del Servicio de Informática.

Artículo 10. Responsable de la Información

1. La figura de Responsable de la Información en lo relativo al ENS, es aquella que tiene la información y determinará sus niveles de seguridad dentro del marco del Esquema Nacional de Seguridad, siendo posible para ello que recabe una propuesta al Responsable de Seguridad, y conveniente que escuche la opinión del Responsable del Sistema.

2. La persona en quien recaerá la figura de Responsable de la Información, y de acuerdo con la guía de seguridad CCN-STIC-801 que trata las responsabilidades y funciones en el ENS, será la persona titular del órgano directivo que tiene la responsabilidad última del uso que se haga de la información y, por tanto, de su protección. En el caso del Defensor del Pueblo Andaluz, la persona Responsable de la Información será la persona titular de la Secretaría General.

3. Los deberes y responsabilidades principales de este perfil de responsabilidad, dentro de su ámbito de actuación y sin perjuicio de otras previstas en el ENS y la guía CCN-STIC-801, son los siguientes:

a) Ayudar a determinar los requisitos de seguridad de la información, identificando los niveles de seguridad de dicha información mediante la valoración del impacto sobre esta de los incidentes que pudieran producirse.

b) Proporcionar la información necesaria 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.

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.

d) Impulsar la adopción de las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado, de acuerdo con el correspondiente análisis de riesgo para los derechos y libertades de las personas físicas y, en su caso, cumplir con las obligaciones establecidas en la presente Política en relativo a la evaluación de impacto.

Artículo 11. Responsables de los Servicios.

1. Los Responsables de los servicios determinarán los niveles de seguridad de los servicios. Tal figura corresponderá a las personas responsables de las áreas/servicios o unidades organizativas que tengan atribuidas competencias técnicas diferenciadas en la tramitación de expedientes de queja y consultas en la Institución. Asimismo, la Secretaría General ostentará la condición de Responsable de los servicios adscritos a la misma, conforme a la estructura organizativa de la Institución.

2. Los deberes y responsabilidades principales de este perfil de responsabilidad, dentro de su ámbito de actuación y sin perjuicio de otras previstas en el ENS y la guía CCN-STIC-801, son los siguientes:

a) Ayudar a determinar los requisitos de seguridad de los servicios a prestar,

identificando los niveles de seguridad de los mismos mediante la valoración del impacto sobre éstos de los incidentes que pudieran producirse.

b) Proporcionar la información necesaria 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.

Artículo 12. Delegado/a de Protección de Datos.

1. El/a Delegado/a de Protección de Datos tiene carácter asesor y supervisor para el cumplimiento de lo dispuesto en el RGPD, en la Ley Orgánica 3/2018, de 5 de diciembre, y demás normativa aplicable sobre protección de datos personales.

2. Sin perjuicio de las funciones que le atribuye el RGPD, en el ámbito de la presente norma, el asesoramiento y supervisión del/la Delegado/a de Protección de Datos se extiendea aquellas medidas de seguridad que se quieran implementar con finalidades distintas a garantizar la protección de datos, en la medida que impliquen un tratamiento adicional de datos personales.

3. Dentro de la gestión general de incidentes, el/la Delegado/A de Protección de Datos intervendrá en la gestión de las brechas de datos personales, principalmente en su posición de interlocutor del Defensor del Pueblo Andaluz y de la Infancia y Adolescencia ante la autoridad de control competente.

Artículo 13. Gestión de los Riesgos.

1. La gestión de riesgos debe realizarse de manera continua sobre los sistemas de información, conforme a los principios de gestión de la seguridad basada en los riesgos, vigilancia continua y reevaluación periódica.

2. El Proceso de Gestión de Riesgos, que comprende la definición de 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 y aprobarse cada año por el CDSI. El Proceso de Gestión de Riesgos aprobado conformará la guía metodológica básica para la elaboración de los respectivos análisis de riesgos, y por lo tanto facilitará la homogenización y comparación de los resultados de cada uno de los análisis de riesgos que se realicen.

3. Las indicadas fases del proceso de gestión de riesgos se realizarán atendiendo a lo dispuesto en los anexos I y II del Real Decreto 311/2022, de 3 de mayo, y siguiendo las normas, instrucciones, guías CCN-STIC y recomendaciones para la aplicación del mismo elaboradas por el Centro Criptológico Nacional.

4. Las personas Responsables de la Información y de los Servicios solicitarán al Responsable de la Seguridad el preceptivo análisis de riesgos para que se proponga el tratamiento adecuado, calculando los riesgos residuales, identificando carencias y debilidades.

5. Se realizará un análisis de riesgos:

a) Regularmente, una vez al año.

b) Cuando haya cambios en los servicios esenciales prestados o cambios significativos en las infraestructuras que los soportan.

c) Cuando ocurra un incidente de seguridad grave.

d) Cuando se identifiquen amenazas severas que no hubieran sido tenidas en cuenta o vulnerabilidades graves que no estén contrarrestadas por las medidas de protección implantadas.

6. La persona Responsable de la Seguridad será la encargada de realizar el análisis de riesgos en tiempo y forma, contando con la colaboración de los correspondientes Responsables de la Información y de los Servicios.

7. Tras la calificación de la información y la determinación de la categoría de seguridad del sistema, se obtendrá la matriz de aplicabilidad y el conjunto de medidas para garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información y del servicio. La evaluación de los riesgos se realizará identificando los riesgos residuales.

8. Será responsabilidad de los Responsables de la Información y de los Servicios, la aceptación de los riesgos residuales y el impulso de la ejecución de auditorías de seguridad.

9. En el caso de que existan tratamientos de datos personales, se deberá tener en cuenta lo dispuesto en el artículo siguiente, de modo que los requisitos identificados conforme a dicho artículo y, con el asesoramiento específico del Delegado de Protección de Datos, se puedan añadir a los establecidos conforme al Real Decreto 311/2022, de 3 de mayo, si así fuera necesario, en particular, fijando el nivel de seguridad a un nivel más alto.

En estos casos, si el resultado del análisis indicara que los tratamientos de datos personales implican un alto riesgo, estos requisitos se elaborarán con la formalidad de una evaluación de impacto en la protección de datos, conforme al artículo 35 del RGPD y los criterios establecidos por la autoridad de control competente. En este aspecto también se deberá tener en cuenta la regulación de la seguridad de los tratamientos de datos personales, especificada en el artículo 32 del RGPD.

Artículo 14. Protección de datos de carácter personal.

1. Se aplicarán a los datos de carácter personal que sean objeto de tratamiento por parte del Defensor del Pueblo Andaluz las medidas de seguridad apropiadas derivadas del análisis de riesgos, así como de la evaluación de impacto relativa a la protección de datos, que se detalla en el RGPD y en la Ley Orgánica 3/2018, de 5 de diciembre.

2. Si del análisis de riesgos y/o la evaluación de impacto en materia de protección de datos se derivara la necesidad de implementar medidas técnicas y/o organizativas más agravadas que las exigidas por la normativa de seguridad, en tal caso prevalecerán las primeras.

Artículo 15. Niveles de desarrollo.

1. El cuerpo normativo 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 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: constituido por la presente Política de Seguridad de la Información.

b) Segundo nivel normativo: constituido por las normas de seguridad derivadas de las anteriores con el objetivo de indicar el uso correcto de aspectos concretos del sistema de gestión de seguridad de la información.

c) Tercer nivel normativo: constituido por procedimientos de seguridad, guías e instrucciones técnicas. Son documentos que, cumpliendo con lo expuesto en la Política de Seguridad de la Información, determinan las acciones o tareas a realizar en el desempeño de un proceso.

2. Además de los documentos citados en el apartado anterior, la documentación de seguridad TIC del dPA podrá contar con otros documentos de carácter no vinculantes como recomendaciones, buenas prácticas, informes, registros, evidencias electrónicas y otros establecidos al respecto.

3. La persona Responsable de Seguridad deberá mantener la documentación de seguridad actualizada y organizada.

4. El CDSI establecerá los mecanismos necesarios para publicar y 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 de seguridad.

Artículo 16. Obligaciones del personal.

1. Todo el personal al servicio del Defensor del Pueblo Andaluz y de la Infancia y Adolescencia de Andalucía, tienen la obligación de conocer y cumplir la presente PSI y su normativa de desarrollo, así como las normas y procedimientos de seguridad aplicables a su ámbito de actuación, siendo responsabilidad del CDSI disponer los medios necesarios para que la información llegue a todas las personas afectadas. Igualmente, esta obligación se aplicará a las personas que ocasionalmente presten servicios o mantengan una relación análoga con la Defensoría.

2. El incumplimiento manifiesto de la PSI o su normativa de desarrollo, así como de los protocolos y procedimientos de seguridad aprobados, podrá acarrear, en su caso, las responsabilidades disciplinarias que correspondan.

Artículo 17. Concienciación y formación.

1. Todo el personal relacionado con la información, los servicios y los sistemas de información, deberá ser formado e informado de sus deberes y obligaciones en materia de seguridad de la información y de protección de datos.

2. Para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios de la Defensoría, se articularán los mecanismos necesarios para llevar a la práctica la concienciación y la formación específica necesaria e imprescindible en todos los niveles de la organización, al menos una vez cada mandato.

Artículo 18. Terceros.

Cuando en el marco de relaciones contractuales, conveniales o análogas el dPA preste o utilice servicios de terceros o a terceros, o cuando obtenga o comunique información de tales terceros o a tales terceros en tales casos les hará participe de esta Política de Seguridad de la Información.

En estos supuestos se establecerán canales de comunicación, coordinación y cooperación entre el dPA y los terceros afectados para el reporte y la coordinación de los respectivos Comités de Seguridad de la Información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando algún aspecto de la Política de Seguridad de la Información del dPA no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y de los servicios afectados antes de llevar a cabo la prestación o utilización de servicios de o a terceros, y antes de obtener o comunicar información de o a tales terceros.

Disposición adicional. Actualización permanente de la Política de Seguridad de la Información.

La PSI de la Defensoría deberá mantenerse actualizada permanentemente para adecuarla a la evolución tecnológica y al desarrollo de la sociedad de la información, así como a los estándares internacionales de seguridad

Disposición derogatoria.

Quedan derogadas cuantas disposiciones de esta Institución se opongan a lo dispuesto en el presente acuerdo.

Disposición final primera.

Las disposiciones de la legislación estatal relativas a la seguridad de la información y, en particular, el Esquema Nacional de Seguridad, se aplicarán como supletorias en las materias regidas por la presente PSI en todo lo no previsto en ella, con las adaptaciones que requiera la organización y funcionamiento propios de la Defensoría y siempre que no resulten contradictorias con las normas por las que la misma se rige.

Disposición final segunda.

Se habilita a la persona titular de la Secretaría General para dictar cuantas instrucciones sean necesarias para la ejecución y desarrollo de lo establecido en la presente Política de Seguridad de la Información.

Disposición final tercera.

La presente Resolución será publicado en el Portal de Transparencia de la Institución y entrará en vigor el día siguiente al de su publicación.