PROPUESTA DE LA SECRETARÍA GENERAL TÉCNICA DE LA CONSEJERÍA DE DERECHOS SOCIALES, IGUALDAD, DIVERSIDAD Y JUVENTUD DE:

PROYECTO DE ORDEN DE LA CONSEJERA DE DERECHOS SOCIALES, IGUALDAD, DIVERSIDAD Y JUVENTUD POR LA QUE SE ESTABLECE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN ESTE DEPARTAMENTO EN EL ÁMBITO DE LA ADMINISTRACIÓN ELECTRÓNICA.

PREÁMBULO

La evolución del ordenamiento jurídico, tanto estatal como autonómico, ha ido incorporando un conjunto de políticas públicas relacionadas, intrínsecamente, con el propio funcionamiento de la Administración y, que por ello, calificadas de instrumentales, tienen todas ellas por finalidad conformar un nuevo modelo de relación del sector público con la ciudadanía que redunde en una prestación de servicios públicos de mayor calidad, más eficaz y eficiente, y adaptado a los nuevos entornos relacionales, como es la relación con la Administración a través de medios digitales, sirviendo mejor a los principios que deben inspirar toda actuación administrativa.

La Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público establece que las Administraciones Públicas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos, que aseguren la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas, garantizarán la protección de los datos de carácter personal, y facilitarán preferentemente la prestación conjunta de servicios a los interesados que recoge el Esquema Nacional de Seguridad, en su artículo 156.

La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas contempla, en su artículo 13, sobre derechos de las personas en sus relaciones con las Administraciones Públicas, el relativo a la protección de datos de carácter personal y, en particular, a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.

En el ámbito de las Administraciones Públicas, la consagración del derecho a comunicarse con ellas a través de medios electrónicos comporta una obligación correlativa de las mismas, que tiene como premisas, la promoción de las condiciones para que la libertad y la igualdad sean reales y efectivas, y la remoción de los obstáculos que impidan o dificulten su plenitud, lo que demanda incorporar las peculiaridades que exigen una aplicación segura de estas tecnologías, promoviendo las

condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, que permita a la ciudadanía y a las Administraciones Públicas el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

Para ello, el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante ENS) viene a derogar 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, estableciendo una regulación actualizada a los notables cambios normativos y a la progresiva transformación digital de nuestra sociedad, adaptándose al nuevo escenario de ciberseguridad y al avance de las tecnologías de aplicación, estableciendo los principios y requisitos de una política de seguridad en la utilización de los medios electrónicos que permita la adecuada protección de la información. Asimismo, en su artículo 12 se dispone que cada Administración Pública contará con una política de seguridad formalmente aprobada por el órgano competente.

En cumplimiento de dicho precepto se ha de aprobar la política de seguridad de este Departamento, adecuándose la misma a la Orden de 31 de julio de 2013, de la Consejería de Presidencia, Justicia e Igualdad, que establece el marco común y las directrices básicas de la política de seguridad de la información en el ámbito de la Administración Electrónica de la Administración Pública de la Comunidad Autónoma.

En la tramitación de esta Orden se ha dado cumplimiento 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. Se han aplicado los principios de necesidad, eficacia y proporcionalidad, en tanto que con la norma se consigue el objetivo perseguido de adaptación a la nueva denominación y estructura organizativa del Departamento. Asimismo se da cumplimiento al principio de seguridad jurídica, al integrarse de forma coherente en el marco normativo autonómico en materia de seguridad jurídica, en el ámbito de la Administración electrónica, facilitando su conocimiento y comprensión por parte de sus destinatarios, así como al principio de transparencia, mediante su publicación en la sede electrónica departamental y al principio de eficiencia, toda vez que evita remisiones administrativas innecesarias o accesorias, y contribuye a una mejor gestión de los recursos públicos.

La norma ha incorporado el enfoque de género en la medida que su ámbito material permite, en cumplimiento de los principios generales que informan la actuación de la Administración Pública y de la Ley 1/2010, de 26 de febrero, canaria de igualdad entre mujeres y hombres, con el uso del lenguaje inclusivo.

La Consejería de Derechos Sociales, Igualdad, Diversidad y Juventud ejerce la gestión de los servicios y competencias que le son propias, en virtud de su correspondiente Reglamento Orgánico, aprobado por el Decreto 43/2020, de 16 de abril, y cualesquiera otras asignadas por las disposiciones vigentes.

En su virtud y, de conformidad con las restantes disposiciones de general aplicación,

DISPONGO:

CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 1.- Objeto y ámbito de aplicación.

1. La presente Resolución tiene por objeto establecer la Política de Seguridad de la Información (en adelante, PSI), en el ámbito de la administración electrónica de la Consejería de Derechos Sociales, Igualdad, Diversidad.

2. La PSI aprobada se aplicará a todos los servicios, aplicaciones o sistemas de la Consejería de Derechos Sociales, Igualdad, Diversidad, por todo el personal de las unidades administrativas de este departamento, así como por el personal de otros organismos o entidades que hayan sido autorizados para acceder a los sistemas de información incluidos en su ámbito de aplicación.

3. La PSI de la de la Consejería de Derechos Sociales, Igualdad, Diversidad debe ser observada por las personas físicas, jurídicas y entes sin personalidad en sus relaciones con las entidades anteriores cuando procedan al uso de sus sistemas de información.

Artículo 2.- Misión del Departamento.

Es misión de la Consejería de Derechos Sociales, Igualdad, Diversidad y Juventud, la propuesta y ejecución de las directrices del Gobierno de Canarias, y de la gestión de los servicios y competencias que le son propias, conforme a su correspondiente Reglamento Orgánico.

Artículo 3.- Principios de la PSI.

Sin perjuicio de los principios básicos establecidos en el ENS, la política de seguridad del Departamento en el ámbito de la administración electrónica se desarrollará, con carácter general, de acuerdo a los siguientes principios:

a) Principio de confidencialidad: los sistemas de información deberán ser accesibles únicamente para aquellas personas usuarias, órganos y entidades o procesos expresamente autorizados para ello, con respeto a las obligaciones de secreto y sigilo profesional.

b) Principio de integridad y calidad: se deberá garantizar el mantenimiento de la integridad y calidad de la información, así como de los procesos de tratamiento de la misma, estableciéndose los mecanismos para asegurar que los procesos de creación, tratamiento, almacenamiento y distribución de la información contribuyen a preservar su exactitud y corrección.

c) Principio de disponibilidad y continuidad: se garantizará un alto nivel de disponibilidad en los sistemas de información y se dotarán de los planes y medidas necesarias para asegurar la continuidad de los servicios y la recuperación ante posibles contingencias graves.

d) Principio de gestión del riesgo: se deberá articular un proceso continuo de análisis y tratamiento de riesgos como mecanismo básico sobre el que debe descansar la gestión de la seguridad de los sistemas de información.

e) Principio de proporcionalidad en coste: la implantación de medidas que mitiguen los riesgos de seguridad de los sistemas de información deberá hacerse bajo un enfoque de proporcionalidad en los costes económicos y operativos.

f) Principio de concienciación y formación: se articularán iniciativas que permitan a las personas usuarias conocer sus deberes y obligaciones en cuanto al tratamiento seguro de la información. De igual forma, se fomentará la formación específica en materia de seguridad TIC de todas aquellas personas que gestionan y administran sistemas de información y telecomunicaciones.

g) Principio de prevención: se desarrollarán planes y líneas de trabajo específicas orientadas a prevenir fraudes, incumplimientos o incidentes relacionados con la seguridad TIC.

h) Principio de mejora continua: se revisará el grado de eficacia de los controles de seguridad TIC implantados, al objeto de adecuarlos a la constante evolución de los riesgos y del entorno tecnológico de la Administración Pública de la Comunidad Autónoma de Canarias.

i) Principio de seguridad TIC en el ciclo de vida de los sistemas de información: las especificaciones de seguridad se incluirán en todas las fases del ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.

j) Principio de función diferenciada: la responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios.

Artículo 4.- Acciones que regirán la PSI.

La PSI del Departamento se sustentará en las siguientes acciones, sin perjuicio de las competencias atribuidas el órgano superior competente en materia de telecomunicaciones y nuevas tecnologías.:

a) La concienciación y la formación del personal adscrito a la Consejería de Derechos Sociales, Igualdad, Diversidad y Juventud, sobre las amenazas y las medidas de seguridad de la información, como acción de participación y corresponsabilidad.

b) El análisis de los riesgos de la seguridad de la información manejada por la Consejería de Derechos Sociales, Igualdad, Diversidad y Juventud, como principio para la prevención de las amenazas a la confidencialidad, la integridad y la continuidad de los servicios públicos prestados a la ciudadanía y a cualquier entidad interesada.

nOZr6S3CqTdVVl773wtxagXMoR7gSDRF

c) La gestión, proactiva o correctiva, de los incidentes de seguridad de la información manejada por la Consejería de Derechos Sociales, Igualdad, Diversidad y Juventud, como principio para la mitigación de sus efectos sobre la confidencialidad, integridad y continuidad de los servicios públicos prestados a la ciudadanía y a cualquier entidad interesada.

d) El cumplimiento por la Consejería de Derechos Sociales, Igualdad, Diversidad y Juventud y sus colaboradores, de la legislación aplicable en materia de telecomunicaciones y nuevas tecnologías, con especial incidencia la relativa de protección de datos de carácter personal, como principio de respeto a los derechos fundamentales de protección de la intimidad y privacidad de la ciudadanía.

e) La medida y el análisis de los indicadores de eficacia y eficiencia de gestión de la seguridad de la información manejada por la Consejería de Derechos Sociales, Igualdad, Diversidad y Juventud, como principio para la innovación y la mejora continua, en este ámbito, de los servicios públicos prestados a la ciudadanía y a cualquier entidad interesada.

Artículo 5.- Definiciones.

A los efectos previstos en esta Orden, las definiciones, palabras, expresiones y términos han de ser entendidos en el siguiente sentido:

a) Gestión de riesgos: actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.

b) Infraestructura tecnológica corporativa: aquellos recursos físicos y lógicos, sobre los que se soportan los sistemas de información, los cuales gestiona el órgano superior competente en materia de telecomunicaciones y nuevas tecnologías.

c) Riesgo: estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.

d) Sistema de Información: conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.

e) Sistemas de Información corporativos: aquellos sistemas de información cuyo ámbito de aplicación y uso es general y común para toda la Administración Pública de la Comunidad Autónoma de Canarias.

f) Sistemas de Información propios: aquellos sistemas de información cuyo ámbito de aplicación es específico para un área concreta y su gestión pertenece a esta Consejería.

nOZr6S3CqTdVVl773wtxagXMoR7gSDRF

Artículo 6.- Marco normativo.

1. El marco normativo para el desarrollo de la gestión de los servicios y competencias de la Consejería es el siguiente:

a) 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).

b)Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantías de Derechos Digitales.

c) Real Decreto 311/2022, de 5 de mayo, por el que se regula el Esquema Nacional de Seguridad.

d) Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

e) Normas Técnicas de Interoperabilidad.

f) Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.

g) Decreto 19/2011, de 10 de febrero, por el que se regula la utilización de los medios electrónicos en la Administración Pública de la Comunidad Autónoma de Canarias.

h) Orden de 31 de julio de 2013, por la que se establece el marco común y las directrices básicas de la política de seguridad de la información en el ámbito de la Administración Electrónica de la Administración Pública de la Comunidad Autónoma de Canarias.

i) Decreto 43/2020, de 16 de abril, por el que se aprueba el Reglamento Orgánico de la Consejería de Derechos Sociales, Igualdad, Diversidad y Juventud, o norma que la sustituya.

j) Acuerdo del Gobierno de Canarias de 25 de junio de 2018 que aprueba las instrucciones que conforman la normativa de seguridad en el uso de los recursos informáticos, telefónicos y de redes de comunicación de la Administración Pública de la Comunidad Autónoma de Canarias.

2. También formarán parte del marco normativo las restantes normas aplicables a la administración electrónica del departamento derivadas de las anteriores, que tendrán consideración de primer nivel normativo conforme a lo previsto en la citada Orden de 31 de julio de 2013.

3. Aparte de las normas del apartado 1, la documentación de seguridad del sistema podrá contar, bajo criterio del Responsable de Seguridad, con otros documentos de carácter no vinculante: recomendaciones, buenas prácticas, informes, registros, evidencias electrónicas, entre otros aspectos.

CAPÍTULO II

ESTRUCTURA ORGANIZATIVA DE LA PSI

Artículo 7.- Organización de la seguridad.

La estructura organizativa de la gestión de la seguridad de la información en el ámbito de la administración electrónica de la Consejería de Derechos Sociales, Igualdad, Diversidad y Juventud está compuesta por los siguientes agentes:

a) El Comité para la Gestión y Coordinación de la Seguridad de la Información.
b) Responsable/s de la Información.
c) Responsable/s de los Servicios Públicos prestados a la Ciudadanía.
d) Responsable de Seguridad de la Información.
e) Responsable/s del Sistema.

Artículo 8.- Comité para la Gestión y Coordinación de la Seguridad de la Información.

1. Se crea el Comité para la Gestión y Coordinación de la Seguridad de la Información (en adelante el Comité), como grupo de trabajo de esta Consejería.

2. El Comité estará compuesto por:

a) Presidencia: la persona titular de la Consejería de Derechos Sociales, Igualdad, Diversidad y Juventud.

b) Vocalías: Las personas titulares de las Direcciones Generales, órganos superiores en los que se estructura el Departamento, la persona titular de la Secretaría General Técnica y el/la Delegado/a de Protección de Datos de la Consejería.

c) Secretaría: una persona con vínculo funcionarial perteneciente a la Secretaría General Técnica, designada por la Presidencia, que actuará con voz y sin voto.

3. El Comité coordinará todas las actividades relacionadas con la seguridad de la información en el Departamento y ejercerá, además de las recogidas en el apartado 3 del artículo 10 de la Orden de 31 de julio de 2013, las siguientes:

a) Supervisar que los procedimientos del sistema de gestión de la seguridad de la información se integran con los procesos de la Consejería, mediante las acciones de auditoría y mejora continua, y responden a los criterios de simplificación, transparencia y agilización administrativa del Gobierno de Canarias.

b) Articular las acciones preventivas y correctivas necesarias para alcanzar los resultados establecidos en los objetivos de seguridad de la información.

c) Impulsar las acciones necesarias de concienciación y la formación del personal adscrito a la Consejería y a las partes interesadas (personas beneficiarias, colaboradoras y entidades proveedoras, etc.) sobre las amenazas y las medidas de seguridad de la información, como principio de participación y corresponsabilidad.

d) Analizar los riesgos de la seguridad de la información manejada por la Consejería, como principio para la prevención de las amenazas a la confidencialidad, la integridad, autenticidad y la continuidad de los servicios públicos que presta.

e) Gestionar, proactiva y correctivamente, los incidentes de seguridad de la información manejada por la Consejería, como principio para la mitigación de sus efectos sobre los servicios públicos que presta.

4. El Comité ajustará su funcionamiento a las previsiones contenidas en la legislación en materia de régimen jurídico del sector público y del procedimiento administrativo común. También podrán aprobar las normas de régimen interno que estime procedentes para el mejor desarrollo de sus trabajos.

5. El Comité se deberá reunir con carácter ordinario, al menos, una vez al año, y con carácter extraordinario cuando lo decida su Presidencia. Las reuniones se realizarán en horario de trabajo y, cuando proceda, por videoconferencia. No se percibirán indemnizaciones en concepto de asistencia por concurrencia al Comité.

6. El Comité podrá recabar de personal técnico la información o asesoramiento pertinente para el ejercicio de sus funciones. En caso necesario este personal podrá ser convocado por el Comité para su asistencia a las reuniones, en calidad de personal asesor, con voz pero sin voto.

7. Podrá acordarse la constitución de subgrupos de trabajo para el análisis, elaboración y ejecución de trabajos o actividades específicas, dentro del ámbito de sus funciones.

Artículo 9.- Responsables de la Información.

1. La Persona Responsable de la Información es aquella que establece las necesidades de seguridad de la información que se maneja y efectúa las valoraciones del impacto que tendría un incidente que afectara a su seguridad.

Tiene además, en exclusiva, la potestad de modificar el nivel de seguridad requerido para la misma.

2. Esta responsabilidad recaerá en la persona titular del órgano que gestione cada procedimiento, trámite o cualquier otro servicio electrónico.

3. Son funciones de cada Persona Responsable de la Información, dentro de su ámbito de actuación, las siguientes:

a) Determinar los niveles de seguridad de la información tratada, valorando los impactos de los incidentes que afecten a la seguridad de la información.

b) Aceptar los riesgos residuales calculados en el análisis de riesgos y realizar su seguimiento y control, junto con las Personas Responsables de los Servicios.

Artículo 10.- Responsables de Servicios.

1. La persona Responsable del Servicio es aquella que determina los requisitos de seguridad de los servicios prestados.

2. Esta responsabilidad recaerá en la persona titular del órgano que gestione cada servicio.

3. Respecto al proceso de gestión del riesgo, las personas responsables de los Servicios Electrónicos son las encargadas, junto a aquellas Responsables de la Información, de aceptar los riesgos residuales calculados en el análisis de riesgos, y de realizar su seguimiento.

Artículo 11.- Responsable de Seguridad.

1. La persona Responsable de Seguridad es aquella que determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

2. Esta responsabilidad recaerá en la persona titular de la Consejería de Derechos Sociales, Igualdad, Diversidad y Juventud.

3. Serán funciones de la persona Responsable de Seguridad las siguientes:

a) Promover la seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información.

b) Proponer la normativa de seguridad de segundo nivel, que según el artículo 15 de la presente Orden, se corresponde con las políticas específicas de seguridad y con las normas STIC, de obligado cumplimiento.

nOZr6S3CqTdVVl773wtxagXMoR7gSDRF

c) Aprobar la normativa de seguridad de tercer nivel, que según el artículo 15 de la presente Orden, se corresponde a los procesos, procedimientos STIC e instrucciones técnicas STIC.

d) Procurar que la documentación de seguridad se mantenga organizada y actualizada, y de gestionar los mecanismos de acceso a la misma.

e) Promover las actividades de concienciación y formación en materia de seguridad en su ámbito de responsabilidad.

f) Realizar la coordinación y seguimiento de la implantación de los proyectos de adecuación al Esquema Nacional de Seguridad.

g) Realizar los preceptivos análisis de riesgos, de seleccionar las salvaguardas a implantar y de revisar el proceso de gestión del riesgo, elevando un informe anual al Comité.

h) Promover auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información, y analizar los informes de auditoría, elaborando las conclusiones a presentar a las personas Responsables del Servicio y de la Información para que adopten las medidas correctoras adecuadas.

i) Coordinar el proceso de Gestión de la Seguridad.

j) Firmar la Declaración de Aplicabilidad, que comprende la relación de medidas de seguridad seleccionadas para un sistema.

k) Elaborar informes periódicos de seguridad que incluyan los incidentes más relevantes en cada período.

l) Determinar la categoría del sistema según el procedimiento descrito en el Anexo I del ENS y las medidas de seguridad que deben aplicarse de acuerdo con lo previsto en el Anexo II del ENS.

m) Proponer la Declaración de Conformidad, para su aprobación por la persona titular del Departamento, previo informe del Comité para la Gestión y Coordinación de la Seguridad de la Información.

n) Verificar que las medidas de seguridad son adecuadas para la protección de la información y los servicios.

4. Cuando la complejidad, distribución, separación física de sus elementos o número de personas usuarias de los sistemas de información lo justifiquen, la persona Responsable de Seguridad podrá designar tantas personas responsables de seguridad delegadas como se necesiten, que tendrán dependencia funcional directa, y que adquirirán responsabilidad en su ámbito de todas aquellas acciones que les sean delegadas.

nOZr6S3CqTdVVl773wtxagXMoR7gSDRF

5. Para el ejercicio de sus funciones podrá contar con el asesoramiento y apoyo del Comité para la Gestión y Coordinación de la Seguridad de la Información.

Artículo 12.- Responsable del Sistema de la Información.

1. Esta responsabilidad recaerá en la persona titular de la Secretaría General Técnica de la Consejería de Derechos Sociales, Igualdad, Diversidad y Juventud como responsable del desarrollo, mantenimiento y explotación del sistema de información que soporte los servicios correspondientes.

2. Los sistemas de información propios de esta Consejería se alojarán en la infraestructura tecnológica corporativa preferiblemente en servidores cibergestionados y, en caso de ser necesario, autogestionados.

3. Serán funciones de la persona Responsable del Sistema las siguientes:

a) Desarrollar, operar y mantener el sistema de Información durante todo su ciclo de vida, así como aprobar los cambios que afecten a la seguridad del modo de operación del sistema.

b) Implantar las medidas necesarias para garantizar la seguridad del sistema durante todo su ciclo de vida, siguiendo las indicaciones de la persona Responsable de Seguridad.

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

d) Suspender el manejo de una determinada información o la prestación de un servicio electrónico si es informado de deficiencias graves de seguridad, previo acuerdo con las personas responsables de dicha información o servicio, y con la de seguridad.

4. Las funciones citadas en el punto anterior podrán recaer en diferentes personas, en el caso de que las competencias sobre los diferentes activos que componen el sistema (aplicaciones, redes, etc.) o las diferentes fases del ciclo de vida del sistema recaigan sobre órganos distintos.

5. Los sistemas de información de la Consejería de Derechos Sociales, Igualdad, Diversidad y Juventud podrán disponer de un Administrador de Seguridad, si fuera preciso, para la mejor gestión de aquellos.

Artículo 13.- Resolución de conflictos.

1. En caso de conflicto entre las diferentes personas responsables que componen la estructura organizativa de la PSI, este será resuelto por el superior jerárquico de los mismos. En su defecto, será resuelto por la persona titular del Departamento, oído el Comité para la Gestión y Coordinación de la Seguridad de la Información.

2. En caso de conflicto entre las personas responsables que componen la estructura organizativa de la PSI y los definidos en seguimiento de la normativa de protección de datos de carácter personal,

prevalecerá la decisión que determine la persona responsable del tratamiento que presente un mayor nivel de exigencia respecto a la protección de los datos de carácter personal.

Artículo 14.- Obligaciones del personal.

1. Todo el personal que presta servicios dentro del ámbito de aplicación de la PSI definido en el artículo 1 de esta Orden, tiene la obligación de conocer y cumplir la PSI, aprobada por la presente Orden, y la normativa de seguridad derivada, siendo responsabilidad del Comité disponer los medios necesarios para que la información llegue a las personas afectadas.

2. Todo el personal que se incorpore o vaya tener acceso a alguno de los sistemas de información o a la información gestionada por ellos deberá ser informado de los términos regulados en esta PSI.

Artículo 15.- Terceras partes.

1. Cuando se presten servicios a otros organismos o se ceda información a terceros:

a) Se les hará partícipes de la PSI y de las normas de seguridad o procedimientos de seguridad relacionados con el servicio o la información afectados.

b) Se establecerán canales de información y coordinación entre los respectivos responsables de gestión de la seguridad de la información y se establecerán procedimientos de seguridad para la reacción ante incidentes.

2. Cuando se utilicen servicios o se maneje información de otros organismos o entidades, se procurarán canales de información y coordinación en materia de seguridad de la información.

3. En los contratos de adquisición de sistemas o aplicaciones informáticas, de prestación de servicios tecnológicos, y también en el caso de contratos de prestación de servicios de otro tipo que implique el uso de servicios, aplicaciones o sistemas informáticos internos, se deberán tener en cuenta las medidas y consideraciones de seguridad de la información que resulten de aplicación, según la legislación vigente en la materia. También se deberán tener en cuenta las medidas y consideraciones de seguridad de la información que resulten de aplicación legal, en caso de acuerdos de cesión de sistemas, aplicaciones o acceso a servicios de otros organismos o entidades.

4. Cuando algún aspecto de la PSI no pueda ser satisfecho por una tercera parte, se requerirá del Responsable de Seguridad un informe sobre los riesgos en que se puede incurrir y la forma de tratarlos. A la vista de dicho informe y antes de que se haga efectiva la prestación, uso, acceso o cesión de que se trate, los responsables de la información o de los servicios afectados decidirán sobre la aceptación o no del riesgo residual.

nOZr6S3CqTdVVl773wtxagXMoR7gSDRF

Artículo 16.- Gestión de 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 y reevaluación periódica.

2. La persona Responsable de Seguridad se encargará de realizar los preceptivos análisis de riesgos, y de seleccionar las salvaguardas a implantar.

3. Las personas Responsables de la Información y de los Servicios se responsabilizarán de los riesgos sobre la información y sobre los servicios, respectivamente y, por tanto, de aceptar los riesgos residuales calculados en el análisis y de realizar su seguimiento y control.

4. 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 cada año por parte de la persona Responsable de Seguridad, que elevará un informe al Comité para la Gestión y Coordinación de la Seguridad de la Información.

Artículo 17.- Desarrollo normativo de la PSI. Documentación de seguridad.

1. El cuerpo normativo sobre seguridad de la información será 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: la Orden de 31 de julio de 2013 por la que se establece el marco común y las directrices básicas de la política de seguridad de la información de la Administración Pública de la Comunidad Autónoma de Canarias, la presente Orden, y las disposiciones generales, directrices y normas de seguridad generales dentro del ámbito de aplicación de la PSI definido en el artículo 1 de esta Orden.

b) Segundo nivel normativo: Políticas Específicas de Seguridad de la Información y Normas de Seguridad TIC (Normas STIC). Las Políticas Específicas desarrollan con un mayor grado de detalle la PSI dentro de un ámbito determinado. Las Normas dan respuesta, sin entrar en detalles de implementación ni tecnológicos, a qué se puede hacer y qué no en relación a un cierto tema desde el punto de vista de la seguridad: qué se considera un uso apropiado o inapropiado, las consecuencias derivadas del incumplimiento, entre otros aspectos. Estas políticas son las aprobadas por el órgano competente en tecnologías de la información del Gobierno de Canarias.

c) Tercer nivel normativo: Procesos y Procedimientos STIC e Instrucciones Técnicas STIC. Son documentos que dan respuesta, incluyendo detalles de implementación y tecnológicos, a cómo se puede realizar una determinada tarea respetando los principios de seguridad de la organización, y los procesos internos en ella establecidos. Serán aprobados por el Comité de Seguridad.

nOZr6S3CqTdVVl773wtxagXMoR7gSDRF

2. Aparte de los documentos citados en el apartado 1, la documentación de seguridad del sistema podrá contar, bajo criterio de la persona Responsable de Seguridad, con otros documentos de carácter no vinculante: recomendaciones, buenas prácticas, informes, registros, evidencias electrónicas, entre otros aspectos.

3. La persona Responsable de Seguridad se responsabilizará de mantener la documentación de seguridad actualizada y organizada, y de gestionar los mecanismos de acceso a la misma.

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

Artículo 18.- Protección de datos de carácter personal.

1. En lo que se refiere a las operaciones de tratamiento de datos de carácter personal, estarán referenciados en el correspondiente registro de operaciones de tratamiento donde se harán constar tanto los ficheros afectados como las personas responsables correspondientes.

2. Todos los sistemas de información de la Consejería de Derechos Sociales, Igualdad, Diversidad y Juventud se ajustarán a los niveles de seguridad requeridos por la normativa de protección de datos de carácter personal. En caso de conflicto con la normativa de seguridad, prevalecerá la norma que presente un mayor nivel de exigencia respecto a la protección de los datos de carácter personal.

Artículo 19.- Formación y concienciación.

1. El Departamento deberá desarrollar actividades formativas específicas orientadas a la concienciación y formación de su personal, así como a la difusión entre el mismo de la PSI y de su desarrollo normativo.

2. El Comité para la Gestión y Coordinación de la Seguridad de la Información y la persona Responsable de Seguridad se encargarán de promover las actividades de formación y concienciación en materia de seguridad.

Artículo 20.- Auditoría.

1. Los sistemas de información propios de esta Consejería y sus organismos autónomos serán objeto, al menos cada dos años, de una auditoría regular ordinaria interna o externa que verifique el cumplimiento de los requerimientos del ENS. 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.

2. Los informes de auditoría quedarán a disposición del Comité para la Gestión y Coordinación de la Seguridad de la Información.

nOZr6S3CqTdVVl773wtxagXMoR7gSDRF

DISPOSICIÓN ADICIONAL

Primera.- Financiación de medidas de cumplimiento de PSI.

La aplicación de las previsiones contenidas en esta Orden, no supondrá incremento del gasto público. Por tanto, los órganos y entidades afectadas deberán desarrollar las medidas derivadas de su cumplimiento ateniéndose a sus disponibilidades presupuestarias ordinarias, no dando lugar, en ningún caso, a planteamientos de necesidades adicionales de financiación.

Segunda.- Facultad para dictar instrucciones de interpretación y aplicación.

Se faculta a la persona titular de la Secretaría General Técnica para dictar las instrucciones que sean necesarias para la correcta interpretación y aplicación de la presente Orden.

DISPOSICIÓN FINAL

Única.- Entrada en vigor.

La presente Orden entrará en vigor el día siguiente al de su publicación en el Boletín Oficial de Canarias.

En Santa Cruz de Tenerife,

LA SECRETARIA GENERAL TÉCNICA

Marlene Santana Rodríguez

nOZr6S3CqTdVVl773wtxagXMoR7gSDRF