DOCUMENTO DE POLÍTICA DE SEGURIDAD TIC EN LA FUNDACIÓN PÚBLICA ANDALUZA PARQUE TECNOLÓGICO DE CIENCIAS DE LA SALUD DE GRANADA

Nombre del fichero	Versión	Resumen de cambios producidos	Fecha
STIC - 01 POLITICA SEG TIC FUNDACIÓN PTS	1.00	Primera versión.	22/06/2020
STIC - 01 POLITICA SEG TIC FUNDACIÓN PTS	2.00	Segunda versión.	03/12/2020
STIC - 01 POLITICA SEG TIC FUNDACIÓN PTS	3.00	Tercera versión.	15/03/2024

INDICE

Fundación Pública Andaluza Parque Tecnológico de Ciencias de la Salud de Granada
Política de Seguridad TIC

I. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 26 de noviembre de 2020 por el Comité de Seguridad TIC.

Esta Política de Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

II. INTRODUCCIÓN

La Fundación Pública Andaluza Parque Tecnológico Ciencias de la Salud de Granada(en adelante Fundación PTS) con NIF Q-1800771-F depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Los diferentes departamentos deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación, deben ser identificados e incluidos en la planificación, en la solicitud de ofertas y en pliegos de licitación para proyectos de TIC.

Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 8 del ENS.

Para el desarrollo de esta Política de seguridad de las tecnologías de la información y las comunicaciones se ha seguido lo dispuesto en: el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS); el Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y

comunicaciones en la Administración de la Junta de Andalucía y su modificación mediante el Decreto 70/2017, de 6 de junio; la Orden de 9 de junio de 2016, por la que se efectúa el desarrollo de la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía.

Adicionalmente, se tienen en cuenta en esta Política de Seguridad los aspectos de seguridad digital requeridos por 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 y en la legislación estatal vigente en materia de protección de datos personales (en adelante, RGPD), y por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

A. PREVENCIÓN

Los departamentos deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello, los departamentos deben implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, los departamentos deben:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

B. DETECCIÓN

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 8 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 9 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

C. RESPUESTA

Los departamentos deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

D. RECUPERACIÓN

Para garantizar la disponibilidad de los servicios críticos, los departamentos deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

III. OBJETO

Esta política se ha de aplicar en el tratamiento de los activos de tecnologías de la información y comunicaciones titularidad de la Fundación Pública Andaluza Parque Tecnológico Ciencias de la Salud de Granada, o cuya gestión tenga encomendada.

IV. ÁMBITO DE APLICACIÓN

El ámbito de aplicación será a todos los servicios de la entidad y así como a todos los miembros de la organización, sin excepciones.

V. MISIÓN

La Fundación Pública Andaluza Parque Tecnológico Ciencias de la Salud de Granada es la entidad gestora del Parque Tecnológico de la Salud de Granada, modelo de transferencia de Investigación y Tecnología básico-clínica en el área de la salud y la biomedicina y que contribuye al desarrollo económico mediante:

- La promoción de una investigación interdisciplinar en biomedicina a nivel internacional para el avance de la salud a través del entendimiento, diagnosis, tratamiento, cura y prevención de enfermedades.
- La protección y transferencia del conocimiento generado especialmente en el área de la salud y la biomedicina.
- La consolidación de un tejido empresarial biosanitario de base tecnológica al servicio de la práctica clínica.
- Ser centro de excelencia asistencial que dé respuesta a las necesidades sanitarias del paciente.

VI. OBJETIVOS, PRINCIPIOS Y DEFINICIONES

Se asumen los principios, objetivos y definiciones establecidos en los artículos 2, 4 y 5 del Decreto 1/2011, de 11 de enero, circunscritos al ámbito competencial de los órganos contemplados en el ámbito de aplicación de esta norma.

1.- Principios básicos.

Los Principios básicos que han de tenerse en cuenta en todas las decisiones que se tomen en materia de seguridad son los establecidos en los artículos 4 a 11 del Real Decreto 311/2022, por el que se regula el Esquema Nacional de Seguridad, y los establecidos en el artículo 5 del Decreto 171/2020, de 13 de octubre, por el que se establece la Política de Seguridad Interior en la Administración de la Junta de Andalucía.

2.- Principios específicos.

Para el cumplimiento de los principios básicos, recogidos en el ENS, se concretan una serie de principios particulares que inspiran las actuaciones de la Fundación PTS y son los siguientes:

a) Organización e implantación del proceso de seguridad. Este Principio recoge la estructura organizativa establecida en el Decreto 171/2020, de 13 de octubre por el que se establece la Política de Seguridad Interior en la Administración de la Junta de Andalucía, cuyo objetivo es facilitar una futura convergencia entre la seguridad física y la ciberseguridad.

b) Análisis y gestión de los riesgos.Se empleará la metodología reconocida internacionalmente y utilizada en el resto de organismos de la Junta de Andalucía. Las medidas adoptadas mitigarán o suprimirán los riesgos, siendo justificadas y proporcionadas.

c) Gestión de personal. Todo el personal de la Fundación PTS relacionado con la información y los sistemas, deberá ser formado e informado de sus deberes y obligaciones en materia de seguridad. Sus actuaciones deben ser supervisadas para verificar que se siguen los procedimientos establecidos.

d) Profesionalidad. La seguridad de los sistemas de información estará atendida y será revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida. La Fundación PTS determinará los requisitos de formación y experiencia necesaria del personal para el desarrollo de su puesto de trabajo

e) Autorización y control de los accesos. El acceso a los sistemas de información y a los activos de la Fundación PTS deberá ser controlado y limitado al personal, a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, restringiendo el acceso a las funciones permitidas.

f) Protección de las instalaciones. Los sistemas se instalarán en áreas separadas, dotadas de un procedimiento de control de acceso. Las salas estarán cerradas y dispondrán de un control de llaves.

g) Adquisición de productos de seguridad y contratación de servicios de seguridad. La Fundación PTS adquirirá productos de seguridad de las tecnologías de la información y comunicaciones que se vayan a utilizar de forma proporcionada a la categoría de los sistemas y su nivel de seguridad.

h) Mínimo privilegio. Los sistemas de información deben diseñarse y configurarse otorgando los mínimos privilegios necesarios para su correcto desempeño

i) Integridad y actualización del sistema. La Fundación PTS deberá conocer el estado de seguridad de los sistemas: especificaciones, vulnerabilidades y actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos.

j) Protección de la información almacenada y en tránsito. La Fundación PTS dispondrá de procedimientos *que* aseguren la recuperación y conservación de los documentos electrónicos y la información en soporte no electrónico, deberá estar protegida con el mismo grado de seguridad que ésta, de conformidad con las normas de aplicación a la seguridad de los mismos.

k) Prevención ante otros sistemas de información interconectados. Se protegerá el perímetro de los sistemas de información de la Fundación PTS reforzando las tareas de prevención, detección y respuesta a incidentes de seguridad.

l) Registro de la actividad y detección de código dañino. La Fundación PTS registrará las actividades de los usuarios, reteniendo la información estrictamente necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

m) Incidentes de seguridad. La Fundación PTS dispondrá de procedimientos de gestión de incidentes de seguridad y de debilidades detectadas en los elementos del sistema de información, o los activos. Estos procedimientos cubrirán los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.

n) Continuidad de la actividad. Los sistemas de la Fundación PTS dispondrán de medidas de respaldo y establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo.

ñ) Mejora continua del proceso de seguridad. El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua. Para ello, la Fundación PTS aplicará los criterios y métodos reconocidos en la práctica nacional e internacional relativos a gestión de las tecnologías de la información.

VII. CONTEXTO TECNOLÓGICO Y RESPONSABILIDAD GENERAL

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

2. La preservación de la seguridad TIC será considerada objetivo común de todas las personas al servicio de los órganos contemplados en el ámbito de aplicación de esta norma, siendo estas responsables del uso correcto de los activos TIC puestos a su disposición.

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

4. Con carácter general, para el personal de Fundación PTS, regirán las normas de uso de los recursos TIC previstas en 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, o en la normativa de carácter horizontal vigente en cada momento.

5. Las normas de uso de los recursos TIC serán trasladadas convenientemente, en la medida en que pueda resultar necesario o recomendable, al clausulado de los contratos suscritos por Fundación PTS.

VIII. MARCO NORMATIVO

La Fundación se rige por la Ley y demás disposiciones de Desarrollo y por la voluntad de sus fundadores, manifiestan en sus estatutos.

El régimen jurídico básico de la Fundación PTS está previsto en la Ley 10/2005, de 31 de mayo, de Fundaciones de la Comunidad Autónoma de Andalucía, en la Ley 9/2007, de 22 de octubre de la Administración de la Junta de Andalucía, en la Ley General de Hacienda Pública de la Junta de Andalucía y en las previsiones que anualmente se recogen en la Ley de Presupuesto de la Comunidad Autónoma de Andalucía para las entidades del sector público.

En materia de presupuestos, contabilidad y auditorías de cuentas, principios a los que ha de sujetarse la selección de personal, régimen de contratación y disposición dineraria de fondos se estará a lo dispuesto en el artículo 57 de la Ley 10/2005 de 31 de mayo de Fundaciones de la comunidad Autónoma de Andalucía.

El personal al servicio de la Fundación PTS se rige por el derecho laboral. El nombramiento del personal no directivo irá precedido de convocatoria pública en medios oficiales y de los procesos selectivos correspondientes basados en los principios de igualdad mérito y capacidad. El personal se sujetará a la normativa sobre retribuciones y condiciones de trabajo del personal del sector público andaluz.

A nivel de Seguridad TIC y Protección de datos, la Fundación PTS desarrollará sus funciones en el marco normativo vigente sin perjuicio de aquella normativa específica que le sea de aplicación por razón del tipo de infraestructuras, servicios o funciones incluidas dentro del marco competencial de la Fundación PTS. En general la normativa aplicable es la siguiente:

- Real Decreto 311/2022 de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS).
- Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía y su modificación parcial mediante Decreto 70/2017, de 6 de junio. y el Decreto 171/2020, de 13 de octubre, por el que se establece la Política de Seguridad Interior en la Administración de la Junta de Andalucía.
- 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) (en adelante, RGPD).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

- Resolución de 22 de octubre de 2020, de la Secretaría General para la Administración Pública, por la que se aprueba el Código de Conducta en el uso de las Tecnologías de la Información y la Comunicación para profesionales públicos de la Administración de la Junta de Andalucía.

IX. ORGANIZACIÓN DE LA SEGURIDAD

1. La gestión de la seguridad de la información en un organismo va íntimamente ligada al establecimiento de una organización de seguridad. Dicha organización se establece mediante la identificación de las diferentes actividades y responsabilidades en materia de gestión de la seguridad y mediante su asignación formal a los agentes que correspondan, con arreglo al principio básico de función diferenciada recogido tanto en el ENS como en la política de seguridad TIC de la Junta de Andalucía.

2. Atendiendo a dicho principio, la estructura que se define en este documento diferencia tres grandes bloques de responsabilidad: a) la especificación de las necesidades y requisitos en materia de seguridad de la información; b) el desarrollo y/o explotación del sistema de información y c) la función de supervisión de la seguridad del sistema de información. En este sentido, los distintos bloques de responsabilidad mencionados quedarán distribuidos como se indica a continuación:

A. Responsables de la información y de los servicios y procedimiento de designación y renovación

1. Los Responsables de la información y/o de los servicios serán las personas titulares de los centros directivos que decidan sobre la finalidad, contenido y uso de la información y/o sobre las características de los servicios a prestar, así como las que determinen los niveles de seguridad dentro del marco establecido en el anexo I del ENS.

2. En virtud del artículo 10.4 del Decreto 1/2011, de 11 de enero, los deberes y responsabilidades principales de estos perfiles 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 y/o de los servicios a prestar,identificando los niveles de seguridad de la información y/o servicios mediante la valoración del impacto sobre los mismos de los incidentes que pudieran producirse.

b) Proporcionar la información necesaria al 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 del Responsable del Sistema (o los responsables si hubiere varios).

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

3. El nombramiento o renovación de estas figuras responsables se realiza en virtud de la presente política de seguridad TIC.

B. Responsable del Sistema y procedimiento de designación y renovación

1. La figura de Responsable del sistema, desde la perspectiva del ENS, de cada sistema de información que se encuentre albergado en los servidores corporativos de la misma será asumida por una persona adscrita a la Gerencia de la Fundación PTS.

2. En virtud del artículo 10.4 del Decreto 1/2011, de 11 de enero, la presente política establece que los deberes y responsabilidades de este perfil de responsabilidad serán los previstos en el ENS y la guía CCNSTIC-801 para la figura del Responsable del Sistema y su designación y renovación se realizará por decisión del Comité de Seguridad de la Fundación PTS y se comunicará, mediante acto documentado, a la persona o personas designadas.

3. La figura de Responsable del sistema, desde la perspectiva del ENS, de los sistemas de información cuya implantación, explotación y mantenimiento se haga fuera de la Fundación PTS, será nombrada o renovada por el responsable de la información o el responsable de servicio correspondiente y se comunicará mediante acto documentado.

C. Responsable Seguridad TIC

1. En virtud del artículo 11.2 del Decreto 1/2011, de 11 de enero, la Fundación PTS contará con un Responsable de Seguridad TIC, garantizando el cumplimiento del principio de función diferenciada recogido en el artículo 5.j) de dicho Decreto. A estos efectos, estará adscrito a la Gerencia de la Fundación PTS.

2. La figura del Responsable de Seguridad TIC de la Fundación PTS nombrada o renovada y se comunicará, mediante acto documentado, por el Comité de Seguridad TIC de este organismo.

3. El Responsable de Seguridad TIC de la Fundación PTS tendrá las atribuciones que establece el artículo 11.2 del Decreto 1/2011, de 11 de enero.

4. El 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, responsable del sistema y responsable de seguridad. Dicho listado se entregará, actualizado, al Comité de Seguridad TIC del organismo en cada una de sus reuniones, con indicación de aquellas deficiencias o faltas de información que se produzcan, de modo que el Comité disponga de información completa y pueda arbitrar los mecanismos necesarios para la subsanación de las deficiencias o faltas de información.

X. COMITÉ DE SEGURIDAD INTERIOR Y SEGURIDAD TIC

1. Se crea el Comité de Seguridad TIC de Fundación PTS como órgano no colegiado de dirección y seguimiento en materia de seguridad de los activos TIC de los que Fundación PTS sea titular o cuya gestión tenga encomendada.
2. Se asume como marco regulador en materia de seguridad interior el establecido por el Decreto 171/2020, de 13 de octubre, y sus posteriores normas de desarrollo y por lo tanto las obligaciones establecidas en el mismo serán asumidas por el Comité de Seguridad TIC, cuya denominación será la de Comité de Seguridad Interior y Seguridad TIC.

El Comité de Seguridad Interior y Seguridad TIC estará formado por:

- Presidencia.
- Secretario.
- Responsable de Información y de los Servicios
- Responsable del Sistema.
- Responsable de Seguridad TIC.
- Delegado de Protección de datos.

2. El Secretario del Comité de Seguridad será el Responsable de Seguridad TIC y tendrá como funciones las indicadas anteriormente.

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

4. Serán funciones propias del Comité de Seguridad Interior y Seguridad TIC serán:

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

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

c) Nombramiento del Responsable de Seguridad TIC de la Fundación PTS.

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

e) Aprobación de la normativa de seguridad TIC de segundo y tercer nivel de la Fundación PTS.

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

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

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

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

j) Impulsar la determinación de los niveles de seguridad de la información tratada, en la que se valorarán los impactos que tendrían los incidentes que afectan a la seguridad de la información,todo ello con la participación de los responsables de la Información correspondientes y del Responsable de Seguridad TIC.

k) Impulsar los preceptivos análisis de riesgos, junto a los responsables de las Informaciones /Servicios que correspondan, contando con la participación de la Unidad /Responsable de Seguridad TIC.

l) Coordinar la aceptación de los riesgos residuales por sus responsables correspondientes respecto dela información / servicios de su competencia, obtenidos en el análisis de riesgos.

m) Asegurar el funcionamiento como sistema eficaz, eficiente y explícitamente definido, de toda la actividad que la Administración de la Junta de Andalucía despliegue para la prevención de daños intencionales sobre su personal y personas usuarias, sobre sus activos y sobre la continuidad de su funcionamiento y servicios, así como para la reacción cuando tales daños se produzcan.

n) Garantizar el cumplimiento de toda la normativa que sea de aplicación a las actuaciones de la Administración de la Junta de Andalucía en esta materia.

ñ) Colaborar a la seguridad a través de la protección del personal, personas usuarias y activos de la Administración de la Junta de Andalucía.

5. El Comité se reunirá al menos una vez al año, previa convocatoria y, de sus reuniones, se levantará acta.

6. El Comité de Seguridad contará con un esquema de suplencias en caso de que las personas titulares no puedan acudir a las reuniones del mismo, cubriendo sus funciones por parte de la persona suplente de forma puntual.

XI. Resolución de conflictos

1. En caso de conflicto entre los diferentes responsables, éste será resuelto por la Gerencia de la Fundación PTS. En defecto de lo anterior, prevalecerá la decisión del Comité de Seguridad.

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

XII. DATOS DE CARÁCTER PERSONAL

Para el tratamiento de datos de carácter personal en los sistemas de información se seguirá en todo momento lo establecido en el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas, en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y en la restante legislación nacional y autonómica vigente en cada momento en relación con esta materia.

2. La seguridad de los datos de carácter personal se basará en criterios de reducción del riesgo dependiendo de la naturaleza y tratamientos de los mismos.

3. Los Responsables de la Información y de los Servicios serán también los responsables de valorar el nivel de seguridad requerido por los sistemas que intervienen en las actividades de tratamiento de datos de carácter personal.

La Fundación PTS trata datos de carácter personal. El documento de seguridad, al que tendrán acceso sólo las personas autorizadas, recoge los ficheros afectados y los responsables correspondientes. Todos los sistemas de información de Fundación PTS se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Documento de Seguridad.

XIII. GESTIÓN DE RIESGOS

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

2. Los responsables de la información, de los servicios y de los tratamientos de datos de carácter personal, en su caso, son responsables de los riesgos sobre los mismos y, por tanto, de aceptar los riesgos residuales calculados en el análisis de riesgos, así como de realizar su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.

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

4. La selección de las medidas de seguridad a aplicar será propuesta por el Responsable de seguridad TIC al Comité de Seguridad, así como el seguimiento de su aplicación. Dichas medidas serán las mínimas determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos que cumpla los requisitos del ENS y de la normativa en materia de protección de datos de carácter personal.

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

6. Para realizar el análisis de riesgos se utilizará la metodología MAGERIT, aprobada por el Consejo Superior de Administración Electrónica, y las herramientas que la apliquen, como PILAR, desarrollada por el Centro Criptológico Nacional.

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- regularmente, al menos una vez al año.
- cuando cambie la información manejada.
- cuando cambien los servicios prestados.
- cuando ocurra un incidente grave de seguridad.
- cuando se reporten vulnerabilidades graves.

Para la armonización de los análisis de riesgos, el Comité de Seguridad TIC establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes

servicios prestados. El Comité de Seguridad dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

XIV. DESARROLLO NORMATIVO DE LA POLÍTICA DE SEGURIDAD

Esta Política de Seguridad de la Información complementa las políticas de seguridad de la Fundación en diferentes materias:

- Listar referencias a otras políticas en materia de seguridad. – Protección de datos.

Esta Política se desarrollará por medio de normativa de seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

Para su mejor difusión entre el personal de la organización y de otras partes interesadas la normativa de seguridad y la política de seguridad estará disponibles en la intranet URL – /Comunes/seguridad TIC.

XV. GESTIÓN DE INCIDENTES DE SEGURIDAD Y DE LA CONTINUIDAD

1. La Fundación PTS deberá estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, según los términos previstos en el artículo 8 del ENS 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.

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

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

XVI. OBLIGACIONES DEL PERSONAL

Todos los miembros de la Fundación PTS tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad TIC disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de la Fundación PTS atenderán a una sesión de concienciación en materia de seguridad TIC al menos una vez al año. Se establecerá un programa de concienciación

continua para atender a todos los miembros de la Fundación, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

XVII. TERCERAS PARTES

Cuando la Fundación PTS preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad TIC y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando la Fundación PTS utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que atañe a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política 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 los servicios afectados antes de seguir adelante.

XVIII. AUDITORÍAS Y CONFORMIDAD CON LA NORMATIVA

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

Los sistemas de información de Fundación PTS serán objeto, al menos cada dos años, de una auditoría regular ordinaria interna o externa que verifique el cumplimiento de los requisitos del ENS y de cualquier otra norma que requiera la realización de auditorías periódicas.

El Responsable de realizará o, en su caso, coordinará, estas actividades de auditoría.

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.

Los informes de auditoría quedarán a disposición del <órgano de dirección> y del Comité de Seguridad TIC.

Por otra parte, el Responsable de seguridad TIC, deberá analizar dicho informe y elevar al Comité de Seguridad TIC las conclusiones que procedan para que éste adopte las medidas correctoras adecuadas.

XIX. 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 la Junta de Andalucía
- Consejo de Transparencia y Protección de Datos de Andalucía
- CCN-CERT: Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional (CCN), como soporte y coordinación para la resolución de incidentes que sufra la Administración General, Autonómica o Local.
- Agencia Española de Protección de Datos (AEPD)
- Instituto Nacional de Ciberseguridad (INCIBE)
- Grupo de Delitos Informáticos y Telemáticos de la Guardia Civil y Brigada de Investigación Tecnológica (BIT) del Cuerpo Nacional de Policía, para la investigación de acciones relacionadas con la delincuencia informática y los fraudes en el sector de las telecomunicaciones.

En Granada a 15 de marzo 2024
Fdo: Luis González Ruiz