Junta de Andalucía

Consejería de Salud y Consumo
Fundación Progreso y Salud

Política de Seguridad Interior

HISTORIAL DE CAMBIOS

NOMBRE DEL FICHERO	VERSIÓN	RESUMEN DE CAMBIOS PRODUCIDOS	FECHA
ITSEC-FPS-Política de Seguidad v1.0.docx	1.0	Primera versión borrador	09/07/2020
ITSEC-FPS-Política de Seguridad Interior 2.0.docx	2.0	Adecuación al 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. Revisión conforme normativa de Política de Seguridad del ENS	Fecha firma electrónica
ITSEC-FPS-Política de Seguridad Interior 3.0.docx	3.0	Actualización RD 3/2010 a RD 311/2022 Modificación de Comité Técnico de Seguridad a Comité Delegado de Seguridad por alineado con el PSI.	Fecha firma electrónica

REFERENCIAS

DOCUMENTOS INTERNOS	
Título	**Nombre del fichero**
Marco Normativo de Seguridad	SGENS -NORM- Elaboración del Marco Normativo de Seguridad.pdf

DOCUMENTOS EXTERNOS
1. Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
2. 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).
3. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
4. 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.
5. CCN-STIC 804. Esquema Nacional de Seguridad. Guía de Implantación.
6. CCN-STIC-821 Normas de Seguridad en el ENS y sus Anexos.
7. CCN-STIC-833 Implantación del ENS para Entidades Locales.
8. Política de Seguridad TIC de la Consejería de Salud y Familias.
9. Política de Seguridad de la Información para el Sistema Sanitario Público de Andalucía (SSPA).

CUMPLIMIENTO	
ENS	**RGPD**

ÍNDICE DE CONTENIDOS

1. INTRODUCCIÓN 5
2. OBJETIVO Y ÁMBITO DE APLICACIÓN 5
3. LEGISLACIÓN Y NORMATIVA DE REFERENCIA 6
4. PRINCIPIOS Y DIRECTRICES 7
4.1. PRINCIPIOS BÁSICOS DEL ENS 7
4.1.1. SEGURIDAD COMO PROCESO INTEGRAL 7
4.1.2. GESTIÓN DE LA SEGURIDAD BASADA EN LOS RIESGOS 8
4.1.3. PREVENCIÓN, DETECCIÓN, RESPUESTA Y CONSERVACIÓN 8
4.1.4. VIGILANCIA CONTINUA Y REEVALUACIÓN PERIÓDICA 8
4.1.5. DIFERENCIACIÓN DE RESPONSABILIDADES 8
4.2. REQUISITOS MÍNIMOS DE SEGURIDAD 8
5. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 11
5.1. COMITÉS DE SEGURIDAD INTERIOR 11
5.2. UNIDAD DE SEGURIDAD INTERIOR 13
5.3. RESPONSABLE DE SEGURIDAD 14
5.4. RESPONSABLES DE LA INFORMACIÓN Y DE LOS SERVICIOS 15
5.5. RESPONSABLE DEL SISTEMA DE INFORMACIÓN 16
5.6. DELEGADO DE PROTECCIÓN DE DATOS 17
5.7. RESPONSABLE DEL TRATAMIENTO 19
5.8. RESOLUCIÓN DE CONFLICTOS 19
5.9. OBLIGACIONES DEL PERSONAL 20
6. ASESORAMIENTO ESPECIALIZADO EN MATERIA DE SEGURIDAD 20
6.1. ASESORAMIENTO ESPECIALIZADO 20
6.2. COOPERACIÓN ENTRE ORGANISMOS Y OTRAS ADMINISTRACIONES PÚBLICAS 20
6.3. REVISIÓN INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN 20
7. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL 20
8. FORMACIÓN Y CONCIENCIACIÓN 21
9. ANÁLISIS Y GESTIÓN DE RIESGOS 21
10. GESTIÓN DE INCIDENTES DE SEGURIDAD Y DE LA CONTINUIDAD. 22
11. INSTRUMENTOS DE DESARROLLO Y ESTRUCTURA NORMATIVA 22
11.1. PRIMER NIVEL: POLÍTICA DE SEGURIDAD INTERIOR Y DIRECTRICES Y NORMAS GENERALES DE SEGURIDAD TIC. 23

11.2. SEGUNDO NIVEL: NORMATIVAS DE SEGURIDAD 23
11.3. TERCER NIVEL: PROCEDIMIENTOS DE SEGURIDAD 23
11.4. CUARTO NIVEL: INFORMES, REGISTROS Y EVIDENCIAS ELECTRÓNICAS 23
11.5. OTRA DOCUMENTACIÓN 23
12. SEGURIDAD DE LA INFORMACIÓN 25
13. OBLIGACIONES DEL PERSONAL 25
14. TERCERAS PARTES 25
15. PUBLICACIÓN DE LA POLÍTICA DE SEGURIDAD 26
16. ENTRADA EN VIGOR 26

1.1.1. Introducción

La Fundación Progreso y Salud, en adelante FPS o simplemente la organización, está adscrita a la Política de Seguridad de las Tecnologías de la Información y de las Comunicaciones (en adelante TIC) de la Consejería de Salud y Familias. No obstante lo anterior, para aquellos sistemas de información que gestione la FPS por cuenta del Servicio Andaluz de Salud y resto de Agencias y entidades adscritas a la Consejería de Salud y Familias, será de aplicación también lo establecido en la Política de Seguridad de la Información del Sistema Sanitario Público de Andalucía.

La FPS, al objeto de implementar en la organización lo establecido en dichas políticas, y como muestra de compromiso con la seguridad de la información de sus sistemas ha desarrollado la presente Política de Seguridad de la Información, en adelante Política de Seguridad, de conformidad con lo establecido en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

La Política de Seguridad TIC de la FPS complementa y desarrolla internamente lo dispuesto en la Política de Seguridad TIC de la Consejería de Salud y Familias, por lo que se estará en todo caso a lo dispuesto en esta última en todo aquello que sea de aplicación a la FPS y que pueda no estar reflejado en este documento.

La Política de Seguridad es una declaración ética, responsable y de estricto cumplimiento en toda la organización, la cual es desplegada a través de las diferentes Normativas y Procedimientos con los que se procura que los riesgos sean tratados adecuadamente.

El uso de los activos de información debe estar en consonancia con las buenas prácticas y procedimientos de trabajo profesionales, así como con los requisitos legales, reglamentarios y contractuales, que deben garantizar la Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad de la información y los servicios.

1.1.2. Objetivo y ámbito de aplicación

La Política de Seguridad persigue la consecución de los siguientes objetivos:

a. Garantizar a los ciudadanos que los datos alojados en FPS serán gestionados de acuerdo a los estándares y buenas prácticas en seguridad.
b. Aumentar el nivel de concienciación en materia de seguridad allí donde es de aplicación esta Política de Seguridad, garantizando que el personal a su servicio es consciente de sus obligaciones y responsabilidades.
c. Establecer las bases de un modelo integral de gestión de la seguridad en FPS, que cubra en un ciclo continuo de mejora los aspectos técnicos, organizativos y procedimentales.
d. Hacer patente el compromiso de FPS con la seguridad de la información mediante su apoyo al Comité de Seguridad dotándole de los medios y facultades necesarias para la realización de sus funciones.
e. Definir, desarrollar y poner en funcionamiento los controles metodológicos técnicos, organizativos y de gestión, necesarios para garantizar de un modo efectivo y medible la preservación de los niveles de confidencialidad, disponibilidad e integridad de la información aprobados por FPS.

f. Garantizar la continuidad de los servicios ofrecidos por FPS a los ciudadanos.
g. Crear y promover de manera continua una “cultura de seguridad” tanto internamente, a todo el personal, como externamente a los ciudadanos y proveedores que permita asegurar la eficiencia y eficacia de los controles implantados y aumente la confianza de nuestros ciudadanos.

Ámbito de aplicación:

Esta Política de Seguridad Interior, será de aplicación y de obligado cumplimiento para todos los Departamentos y Servicios de FPS, entendiendo por Departamentos y Servicios a sus Líneas de actividad, Áreas, Unidades y estructuras gestionadas por la Fundación; a sus recursos y a los procesos afectados por el ENS y el RGPD, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

Este documento constituye el establecimiento de un marco organizativo y tecnológico en la organización.

Se entenderá la Seguridad, como un proceso integral constituido por todos los elementos técnicos, humanos y materiales y organizativos relacionados con los sistemas de información, quedando excluidas cualquier tipo de actuaciones puntuales o de tratamiento coyuntural.

Debe ser conocida y cumplida por todo el personal de la organización, independientemente del puesto, cargo y responsabilidad dentro del mismo, así como por el personal que en el ámbito de las actividades subcontratadas con terceros tenga acceso a los sistemas de información de FPS.

1.1.3. Legislación y normativa de referencia

El marco normativo de las actividades de FPS en el ámbito de esta Política de Seguridad está integrado por las siguientes normas:

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- 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.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- 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)
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

- Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.
- Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.
- 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.
- Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
- Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (Reglamento eIDAS).
- Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
- Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía.
- 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.
- 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
- Orden de la Consejería de Empleo, Empresa y Comercio, 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.

1.1.4. Principios y directrices

La Política de Seguridad de FPS se desarrollará, con carácter general, de acuerdo a los siguientes principios:

1.1.5. Principios básicos del ENS

4.1.1. Seguridad como proceso integral

La seguridad se entiende como un proceso integral constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con el sistema de información. Se prestará atención a la concienciación de las personas para evitar que la ignorancia, la falta de organización y de coordinación, constituyan fuentes de riesgo.

4.1.2. Gestión de la seguridad basada en los riesgos

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 activos TIC.

4.1.3. Prevención, detección, respuesta y conservación

Se desarrollarán planes y líneas de trabajo específicas orientadas a prevenir fraudes, incumplimientos o incidentes relacionados con la seguridad. De igual manera, el sistema mantendrá disponibles los servicios durante todo el ciclo vital de la información digital.

4.1.4. Vigilancia continua y reevaluación periódica

La vigilancia continua detectará actividades anómalas a las que dará respuesta. Los controles de seguridad implantados, se reevaluarán al objeto de adecuar su eficacia a la constante evolución de los riesgos, de los sistemas de protección y del entorno tecnológico.

4.1.5. Diferenciación de responsabilidades

La responsabilidad de la seguridad de los sistemas estará diferenciada de la responsabilidad de seguridad, así como de la responsabilidad de la información y la responsabilidad del servicio. Los roles y responsabilidades de cada una de estas funciones deberán quedar debidamente acotadas y reflejadas documentalmente.

4.1.6. Existencia de líneas de defensa

La estrategia de seguridad de la entidad se diseña e implementa en capas de seguridad.

1.1.6. Requisitos mínimos de seguridad

Esta Política de Seguridad Interior se establecerá de acuerdo con los principios básicos indicados y se desarrollará aplicando los siguientes requisitos mínimos:

a. Organización e implantación de un Sistema de Gestión de seguridad: la seguridad de los sistemas de información compromete a todos los miembros de FPS. Así mismo, la estructura organizativa establecida en FPS, cumplirá el principio de Diferenciación de Responsabilidades.

b. Análisis y gestión de los riesgos: el análisis y gestión de riesgos será parte esencial del proceso de seguridad. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad.

c. Gestión del personal: 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 uso indebido de dichos activos.

d. Profesionalidad: la seguridad de los sistemas estará atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida. El personal recibirá la formación específica necesaria para garantizar la seguridad de las tecnologías de la información aplicables. Se exigirá, de manera objetiva y no discriminatoria, que los prestadores de servicios de seguridad cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados.

e. Autorización y control de los accesos: se limitará el acceso a los activos de información por parte de usuarios, procesos, dispositivos 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.

f. Protección de las instalaciones: 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.

g. Adquisición de productos de seguridad y contratación de servicios de seguridad: en la adquisición de productos de seguridad será exigible la certificación de la funcionalidad de seguridad relacionada con el objeto de dicha adquisición, según la categoría del sistema y el criterio del responsable de seguridad. Para la contratación de servicios de seguridad se estará obligado a lo dispuesto en el principio de profesionalidad.

h. Mínimo privilegio: lo sistemas de información se diseñarán y configurarán otorgando los mínimos privilegios necesarios para su correcto desempeño.

i. Integridad y actualización del sistema: la inclusión de elementos físicos o lógicos requerirán autorización formal previa a su instalación en el sistema. También para cualquier modificación de la configuración de hardware y software.

j. Protección de la información almacenada y en tránsito: se prestará especial atención a la información almacenada o en tránsito a través de entornos inseguros, como los equipos portátiles, dispositivos portátiles, soportes de información y comunicaciones sobre redes abiertas o con cifrado débil. También forman parte de la seguridad los procedimientos que aseguren la recuperación y conservación a largo plazo de los documentos electrónicos producidos por FPS. Así como la información en soporte no electrónico que haya sido causa o consecuencia de ellos.

k. Prevención ante otros sistemas de información interconectados: se protegerá el perímetro del sistema de información. También se analizará los riesgos derivados de la interconexión de sistemas y se controlará el punto de unión.

l. Registro de actividad y detección de código dañino: Se registrarán las actividades de los usuarios, reteniendo la información 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: se implantarán los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad. Esta gestión de los incidentes se empleará para la mejora continua de la seguridad del sistema.

n. Continuidad de la actividad: 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 a las necesidades de nivel de servicio de sus usuarios.

o. Mejora continua del Sistema de Gestión de seguridad: Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado, instruido y dedicado.

1.1.7. Organización de la seguridad de la información

El mantenimiento y gestión de la seguridad de la información va íntimamente ligado al establecimiento de una organización de seguridad. Dicha organización se establece mediante la identificación y definición de las diferentes actividades y responsabilidades en materia de gestión de la seguridad y la implantación de una estructura que las soporte. La estructura organizativa de la gestión de la seguridad de la información de la Fundación viene a complementar en la organización a la prevista en la Política de Seguridad de la Consejería de Salud y Familias, y contempla una estructura jerárquica de Comités de Seguridad Interior de la Información, y la definición de los diferentes roles y responsabilidades en el gobierno y la gestión de la Seguridad de la Información. En la FPS esta estructura organizativa está compuesta por los siguientes agentes:

a) Comités de Seguridad: Comité de Seguridad Interior y Seguridad TIC y Comité Técnico de Seguridad.
b) Unidad de Seguridad Interior.
c) Responsable de Seguridad.
d) Responsables de la Información y de los Servicios (personas titulares y delegadas).
e) Responsables del Sistema de Información.
f) Delegados/as de Protección de Datos.
g) Responsable del Tratamiento.

Dependiendo de las necesidades y circunstancias de la organización, en ciertos casos, la función de algunos de estos agentes podrá recaer sobre una misma persona, unidad o departamento, siempre que no exista conflicto de intereses.

5.1. Comités de Seguridad Interior

Para la gestión de la Seguridad de la Información, se establece el **Comité de Seguridad Interior y Seguridad TIC**, dentro del ámbito de la presente Política de Seguridad, como órgano de dirección y seguimiento en materia de seguridad interior. Estará formado por:

- La Dirección Gerencia, a cargo de la Presidencia del Comité.
- Las personas responsables de Información o de Servicio, a cargo de las direcciones de las diferentes líneas y áreas de actividad de la FPS.
- La persona Responsable de Seguridad, a cargo de la Dirección de Gestión y Organización Interna y en quien recae la Secretaría del Comité.
- La persona Responsable del Sistema de Información.
- Las personas Delegadas de Protección de Datos de la Consejería de Salud y Familias y del Servicio Andaluz de Salud.

Asimismo, el Comité de Seguridad Interior y Seguridad TIC podrá convocar a sus reuniones a las personas que en cada caso autorice la Presidencia, por propia iniciativa o a propuesta de alguno de sus miembros.

El Comité de Seguridad Interior y Seguridad TIC contará con el soporte interno en materia de protección de datos y seguridad de la información con el técnico auxiliar de Organización de la FPS, en coordinación

con las personas Delegadas de Protección de Datos y podrá recabar de personal técnico especializado, propio o externo, la información pertinente para la toma de decisiones.

Son funciones del Comité de Seguridad Interior y Seguridad TIC las siguientes:

a) Definición, aprobación y seguimiento de los objetivos, iniciativas y planes estratégicos para la seguridad interior, incluido el Plan de Seguridad Interior.
b) Velar por la disponibilidad de los recursos necesarios para desarrollar las iniciativas y planes estratégicos definidos.
c) El establecimiento de directrices comunes y la supervisión del cumplimiento de la normativa de seguridad interior.
d) La aprobación del modelo de relación con los Puntos Coordinadores de Seguridad Interior.
e) La promoción de la educación, el entrenamiento y la concienciación sobre las medidas relativas a la seguridad interior entre el personal.
f) El análisis y la adopción de decisiones en la respuesta a incidentes susceptibles de generar una crisis de seguridad.
g) La designación de la Unidad de Seguridad Interior
h) Las previsiones para la designación de los Puntos Coordinadores de Seguridad Interior
i) Identificar los objetivos de la organización en el ámbito de la Seguridad de la Información.
j) Elaborar la Política de Seguridad, en el marco de la Política de Seguridad TIC de la Consejería de Salud y Familias, establecer los criterios de revisión de la misma, revisarla, distribuirla y velar por su cumplimiento.
k) Promover y respaldar los planes de acción e iniciativas que garanticen la implantación de la Política de Seguridad en la organización.
l) Establecer los requisitos de seguridad que deben cumplir a nivel organizativo, técnicos y de control, los sistemas y servicios de la organización.
m) Garantizar que la seguridad forma parte del proceso de planificación de la gestión de la información y como proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con los sistemas de información.
n) Comunicar a los terceros que colaboren en la explotación de los sistemas de información la realización de la misma conforme a los exigidos en el ENS.
o) Aprobar los nombramientos de responsables y responsabilidades en materia de seguridad de la información. Se aprobará el nombramiento de personas responsables de información o de servicio delegadas, con ámbitos más específicos de actividad, que podrán apoyar a los miembros de los Comités de Seguridad de la FPS.
p) Valorar el grado de conformidad de los procedimientos implantados en la organización con las normas definidas en la política, estableciendo planes de mejora para aquellos que requieran de una modificación para su conformidad.
q) Supervisar las normativas y procedimientos de seguridad que se definan para dar cumplimiento y desarrollo a la Política de Seguridad.
r) Acordar y aprobar metodologías y procesos específicos relativos a la Seguridad de la Información.
s) Verificar que todas las acciones llevadas a cabo en materia de Seguridad sean compatibles o se encuentren respaldadas por la Política de Seguridad.

t) Promover la realización de auditorías periódicas que permitan verificar el cumplimiento de las obligaciones de las Administraciones en materia de Seguridad.
u) Promover la formación y concienciación en materia de Seguridad de la Información a todo el personal.
v) Mantener contactos periódicos con grupos, otras entidades, organismos, foros, etc. que resulten de interés en el ámbito de la Seguridad de la Información, compartiendo experiencias y conocimiento que ayuden a mejorar y mantener la seguridad de los sistemas de la organización.
w) Valorar y evaluar los recursos necesarios para dar soporte al proceso de planificación e implantación de la seguridad en la organización.

El Comité de Seguridad, se reunirá con carácter ordinario, al menos una vez al año, pudiéndose reunir en periodos inferiores. El Comité se reunirá previa convocatoria y de sus reuniones se levantará acta por la Secretaría, que será aprobada en la misma o en la próxima reunión del mismo.

Por su parte, el Comité de Seguridad Interior y Seguridad TIC nombrará asimismo al **Comité Delegado de Seguridad** como órgano de apoyo en el nivel operativo y de supervisión derivado de las funciones a desempeñar.

El Comité Técnico de Seguridad estará compuesto por los siguientes miembros:

- La persona Responsable de Seguridad.
- La persona Responsable de Sistemas.
- Las personas Delegadas de Protección de Datos

Asimismo, el Comité Técnico de Seguridad contará con el soporte interno en materia de protección de datos y seguridad de la información con el técnico auxiliar de Organización de la FPS, en coordinación con las personas Delegadas de Protección de Datos, podrá recabar de personal técnico especializado, propio o externo, la información pertinente para la toma de decisiones y convocará a sus reuniones a las personas Responsables de la Información o de Servicio o a las personas en las que éstas deleguen.

5.2. Unidad de Seguridad Interior

La Unidad de Seguridad, cuyos miembros se designan por el Comité de Seguridad Interior y Seguridad TIC, ejerce la responsabilidad ejecutiva para la seguridad interior del conjunto de los activos en su ámbito.

Le corresponde a esta Unidad las siguientes funciones:

a) Las labores de soporte, asesoramiento e información al Comité de Seguridad Interior y Seguridad TIC, así como la ejecución de sus decisiones y acuerdos en materia de seguridad interior. Propuesta de un Plan de Seguridad Interior para la FPS.

b) Proponer las adaptaciones necesarias del modelo general de seguridad interior, incluso valores, tablas y métricas adecuadas al conjunto de los activos en su ámbito.

c) El desarrollo, el mantenimiento y la supervisión del marco regulador de la seguridad interior en la FPS.

d) La generación y supervisión de criterios y directrices para la gestión de la seguridad interior en el ámbito de la FPS.

e) La recogida sistemática de información y la supervisión del estado de las principales variables de seguridad interior en el ámbito de la FPS.

f) La coordinación y el seguimiento de la actividad de los puntos coordinadores responsables de seguridad interior de la FPS.

g) El asesoramiento técnico y la auditoría del sistema de seguridad interior en la FPS.

h) Velar por la coherencia de la aplicación del modelo de seguridad interior en la FPS, mantenerlo actualizado e impulsar su implantación.

i) Gestionar para la FPS, la relación con la Unidad Corporativa de Seguridad Interior.

j) Definir los criterios de protección de activos especialmente sensibles a riesgos que conciernen a la seguridad interior conforme a las especificidades de la FPS.

k) Desarrollar para la FPS, planes de contingencia en respuesta a incidentes de seguridad interior, incluso situaciones de crisis.

l) Asegurar en la FPS, el funcionamiento de los mecanismos previstos para recopilar, recibir, analizar y procesar la información relevante para la seguridad interior, destinados a generar inteligencia al respecto.

m) Promover y coordinar la cooperación con las autoridades del sector correspondiente al ámbito material de la Consejería o entidad en materia de inteligencia para la seguridad.

n) Informar sobre incidentes de seguridad interior en la Consejería o entidad que se consideren relevantes.

ñ) Asegurar en su nivel el correcto funcionamiento en la cadena de comunicación y escalado de incidentes de seguridad interior.

o) Proponer a la aprobación del Comité de Seguridad Interior y Seguridad TIC el Plan de Seguridad Interior de la Consejería o entidad dependiente singular.

p) Cuantas otras le sean encomendadas en relación con la seguridad interior por el Comité de Seguridad Interior y Seguridad TIC.

5.3. Responsable de Seguridad

Es la persona responsable de supervisar que los servicios y sistemas de información de la organización se mantengan con el mayor grado de seguridad atendiendo a los principios de:

a) Confidencialidad: la información asociada a los servicios electrónicos al ciudadano solo debe poder ser conocida por las personas autorizadas para ello.
b) Integridad: la información asociada a los servicios electrónicos al ciudadano no debe ser alterada por personas no autorizadas.

c) Disponibilidad: garantía de que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma siempre que lo requieran, así como garantía de que los servicios relativos a la Administración Electrónica permanecerán disponibles.

Son funciones de la persona Responsable de Seguridad:

a) Supervisar el cumplimiento de la presente Política, de sus normas y procedimientos derivados.
b) Asesorar en materia de seguridad a los integrantes de FPS que así lo requieran.
c) Coordinar la interacción con otros organismos especializados.
d) Tomar conocimiento y supervisar la investigación y monitorización de los incidentes de seguridad.
e) Coordinar el establecimiento las medidas de seguridad, adecuadas y eficaces para cumplir los requisitos de seguridad establecidos por los responsables de los Servicios y de la Información, siguiendo en todo momento lo exigido en el Anexo II del ENS.
f) Asesorar, en colaboración con el responsable del Sistema, los responsables de los Servicios y de la Información en la realización de los análisis y gestión de riesgos, elevando el informe resultado al Comité de Seguridad.
g) Promover las actividades de concienciación y formación en materia de seguridad en su ámbito de responsabilidad, siguiendo las directrices del Comité de Seguridad.
h) Preparar los temas a tratar en las reuniones del Comité de Seguridad, aportando información puntual para la toma de decisiones.

Respecto a la documentación, son funciones del Responsable de Seguridad:

a) Aprobar y proponer al Comité de Seguridad la documentación de seguridad de segundo nivel (Normativas y Procedimientos de Seguridad) de obligado cumplimiento.
b) Supervisar la documentación de tercer nivel (Procedimientos Técnicos de Seguridad) de obligado cumplimiento.
c) Mantener la documentación organizada y actualizada, gestionando los mecanismos de acceso a la misma.

En aquellos sistemas de información que, por su complejidad, distribución, separación física de elementos o números de usuarios se necesitara de personal adicional para llevar a cabo las funciones del Responsable de Seguridad, el Responsable de Seguridad podrá designar cuantos Responsables de Seguridad Delegados considere necesarios. Los Responsables de Seguridad Delegados se harán cargo, en su ámbito, de todas aquellas acciones que delegue el Responsable de Seguridad teniendo dependencias funcionales directas con él.

El Responsable de Seguridad será nombrado y cesado por el Comité de Seguridad.

5.4. Responsables de la Información y de los Servicios

Esta responsabilidad recaerá, por un lado, en las personas responsables de las líneas y áreas de actividad de la FPS, que gestione cada flujo de información o servicio, pudiendo una misma persona acumular las responsabilidades de la información de todos los procedimientos que gestione. Por otro lado, recaerá

también de forma delegada en personas nombradas por las anteriores, con ámbitos de responsabilidad más específicos (departamentos, sistemas, servicios, etc.).

Son los responsables de clasificar la información conforme a los criterios y categorías establecidas en el ENS y en cada una de las dimensiones de seguridad conocidas y aplicables, dentro del marco establecido en el Anexo I del ENS.

Son los responsables de determinar los niveles de seguridad de los servicios en cada dimensión de seguridad dentro del marco establecido en el Anexo I del ENS y en cada una de las dimensiones de seguridad conocidas y aplicables (disponibilidad, autenticidad, trazabilidad, confidencialidad e integridad).

Son los encargados, contando con la participación y asesoramiento del Responsable de Seguridad y del responsable del Sistema de Información, de realizar los preceptivos análisis de riesgos, y de seleccionar las salvaguardas a implantar.

Son los responsables de aceptar los riesgos residuales calculados en el análisis de riesgos, y de realizar su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.

Asimismo, recaen en las personas responsables de información y servicios las funciones del responsable del tratamiento en el o los tratamientos concretos de la organización que quedan bajo su ámbito de actuación. En concreto son:

- Garantizar la observancia de los principios relativos al tratamiento.
- Garantizar el cumplimiento de las medidas técnicas y organizativas definidas.
- Garantizar el cumplimiento de las políticas y normativas aprobadas e implementadas en la organización.
- Asegurar que la realización de tratamientos por cuenta de terceras partes esté regulada en un contrato, que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que la persona encargada del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará (ni siquiera para su conservación) a otras personas.
- Adoptar las medidas correctoras adecuadas.

Los responsables de información y de los servicios son establecidos en el Plan de adecuación al ENS y Mejora a la Seguridad, el cual contiene la planificación de actuaciones destinadas a subsanar las insuficiencias detectadas, para el cumplimiento del Esquema Nacional de Seguridad.

5.5. Responsable del Sistema de Información

Personal designado cuyas responsabilidades son la supervisión sobre:

a) El desarrollo, operación y mantenimiento del sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
b) Que las medidas de seguridad se integren adecuadamente dentro del marco general de la Seguridad de la Información.

c) La aprobación de toda modificación sustancial de la configuración de cualquier elemento del sistema.
d) La elaboración de procedimientos técnicos de seguridad de los sistemas de información.
e) La elaboración de planes de continuidad de los sistemas de información.

Podrá 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 el responsable de la Información y servicio afectados y el Responsable de Seguridad antes de ser ejecutada.

En aquellos sistemas que, por su complejidad, distribución, separación física de elementos o número de usuarios se necesite personal adicional para llevar a cabo las funciones de Responsable de Sistemas, se podrán designar cuantos Responsables de Sistemas Delegado se consideren oportunos. La designación y delegación de funciones en los Responsables de Sistemas Delegados corresponde al responsable del Sistema, sin perjuicio de que la responsabilidad final siga recayendo sobre el responsable del Sistema. Los Responsable de Sistemas Delegados se harán cargo en su ámbito de todas aquellas acciones que delegue el responsable del Sistema relacionadas con la operación, mantenimiento, instalación y verificación del correcto funcionamiento del Sistema de Información correspondiente, así como también tendrá dependencia funcional directa con el responsable del Sistema que es a quién reporta.

Los responsables del Sistema de Información son establecidos en el Plan Director de Seguridad, el cual contiene la planificación de actuaciones destinadas a subsanar las insuficiencias detectadas, para el cumplimiento del Esquema Nacional de Seguridad. Por regla general será el departamento de Informática, pudiendo delegar en los responsables de cada uno de los sistemas afectados.

5.6. Delegado de Protección de Datos

El Delegado de Protección de Datos será único para todos los órganos y organismos de la organización se informará de su nombramiento y cese a la Agencia Española de Protección de Datos.

Son funciones del Delegado de Protección de Datos:

- Informar y asesorar a la organización y a todos los empleados que se ocupen del tratamiento de datos personales, de las obligaciones que se deriven del Reglamento General de Protección de Datos y de otras disposiciones relacionadas con la protección de datos.
- Supervisar el cumplimiento del Reglamento General de Protección de Datos en la organización.
- Asesorar acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación.
- Cooperar con la Autoridad de control
- Actuar como punto de contacto de la Autoridad de Control

Además, asesorará y supervisará en las siguientes áreas:

- Cumplimiento de principios relativos al tratamiento, como los de limitación en la finalidad, minimización o exactitud de los datos
- Identificación de las bases jurídicas de los tratamientos.

- Valoración de compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos.
- Existencia de normativa sectorial que pueda determinar condiciones de tratamiento específicas distintas de las establecidas por la normativa general de protección de datos.
- Diseño e implantación de medidas de información a los afectados por los tratamientos de datos.
- Establecimiento de mecanismos de recepción y gestión de solicitudes de ejercicio de derechos por parte de los interesados.
- Valoración de las solicitudes de ejercicio de derechos por parte de los interesados.
- Contratación de encargados de tratamiento, incluido el contenido de los contratos o actos jurídicos que regulen la relación organización – encargado de tratamiento.
- Identificación de los instrumentos de transferencia internacional de datos adecuados a las necesidades y características de la organización y de las razones que justifiquen la transferencia.
- Diseño e implantación de políticas de protección de datos.
- Auditorías de protección de datos.
- Establecimiento y gestión de los registros de actividades de tratamiento
- Análisis de riesgo de los tratamientos realizados
- Implantación de las medidas de protección de datos desde el diseño y protección de datos por defecto adecuadas a los riesgos y naturaleza de los tratamientos
- Implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos
- Establecimiento de procedimientos de gestión de violaciones de seguridad de los datos, incluida la evaluación del riesgo para los derechos y libertades de los afectados y los procedimientos de notificación a las autoridades de supervisión y a los afectados
- Determinación de la necesidad de realización de evaluaciones de impacto sobre la protección de datos
- Realización de evaluaciones de impacto sobre la protección de datos
- Relaciones con las autoridades de supervisión
- Implantación de programas de formación y sensibilización del personal de la organización en materia de protección de datos.

La persona designada como delegado/a de Protección de Datos en la FPS se corresponde con la persona titular de este puesto en la Consejería con competencias en materia de Salud, y cuenta para el soporte interno y coordinación de acciones en materia de protección de datos y seguridad de la información con el técnico auxiliar de Organización de la FPS.

5.7. Responsable del Tratamiento

El responsable del tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determina los fines y medios del tratamiento, es decir, FPS en los tratamientos que les corresponda o aquellas entidades que hayan encomendado a la FPS el tratamiento de sus datos personales con arreglo al artículo 28 del 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 adelante Reglamento (UE) 2016/679),.

La FPS debe, entre otras cosas:

- Garantizar la observancia de los principios relativos al tratamiento y aprobar la política, normativa y procedimientos concernientes a la protección de datos personales.
- Designar a quien ejerza como Responsable de Seguridad, quien deberá coordinar y controlar las medidas derivadas de la normativa de protección de datos.
- Designar al Delegado de Protección de Datos, cuando corresponda.
- Adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos personales y evitar su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural. En particular, difundirá entre el personal las normas de seguridad que afecten al desarrollo de sus funciones, así como las consecuencias en que pudieran incurrir en caso de incumplimiento.
- Garantizar el cumplimiento de las políticas y normativas aprobadas e implementadas en la organización.
- Asegurar que la realización de tratamientos por cuenta de terceras partes esté regulada en un contrato, que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que la persona encargada del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará (ni siquiera para su conservación) a otras personas.
- Adoptar las medidas correctoras adecuadas.

5.8. Resolución de conflictos

En caso de conflicto entre los diferentes responsables, éste será resuelto por el órgano superior jerárquico común de los mismos. En defecto de lo anterior, prevalecerá la decisión del Comité de Seguridad Interior y Seguridad TIC.

En los conflictos entre las personas responsables que componen la estructura organizativa de la Política de seguridad TIC de la Consejería de Salud y Familias y de la FPS, 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.

5.9. Obligaciones del Personal

Todo el personal, tanto el de FPS como el de entidades colaboradoras o empresas proveedoras, tiene la obligación de conocer y cumplir la presente Política de Seguridad, las normativas y procedimientos derivados de la misma, tales como las relativas a la protección de datos de carácter personal, siendo responsabilidad del Comité de Seguridad disponer de los mecanismos necesarios para que la información llegue a todo el personal indicado.

El incumplimiento manifiesto de la Política de Seguridad de la Información o la normativa y procedimientos derivados de ésta podrá acarrear el inicio de medidas disciplinarias oportunas y, en su caso, las responsabilidades legales correspondientes.

1.1.8. Asesoramiento especializado en materia de seguridad

6.1. Asesoramiento especializado

El Responsable de Seguridad será el encargado de coordinar los conocimientos y las experiencias disponibles en FPS con el fin de proporcionar ayuda en la toma de decisiones en materia de seguridad, pudiendo obtener asesoramiento de otros organismos.

6.2. Cooperación entre organismos y otras Administraciones Públicas

A efectos de intercambiar experiencias y obtener asesoramiento para la mejora de las prácticas y controles de seguridad, FPS mantendrá contactos periódicos con organismos y entidades especializadas en temas de seguridad.

6.3. Revisión independiente de la Seguridad de la Información

El Comité de Seguridad propondrá la realización de revisiones periódicas independientes sobre la vigencia e implementación de la Política de Seguridad con el fin de garantizar que las prácticas en la organización reflejan adecuadamente sus disposiciones.

1.1.9. Protección de datos de carácter personal

Para el tratamiento de datos de carácter personal en los sistemas de información se seguirá en todo momento lo desarrollado en el documento de seguridad y su documentación asociada conforme a lo exigido en el Reglamento UE 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de

protección de datos); y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

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.

Para el cumplimiento de la obligación de disponer de un registro de tratamientos, se estará a lo indicado en el apartado dedicado al Delegado de Protección de Datos, de la Política de Seguridad TIC de la Consejería de Salud y Familias.

1.1.10. Formación y concienciación

El objetivo es lograr la plena conciencia respecto a que la Seguridad de la Información afecta a todo el personal de la organización y a todas las actividades. A estos efectos, la organización, propondrá y organizará sesiones formativas y de concienciación para que todas las personas que intervienen en el proceso y sus responsables jerárquicos tengan una sensibilidad hacia los riesgos que se corren, conozcan los elementos fundamentales del proceso de Seguridad de la Información y sean conscientes de la responsabilidad que le corresponde al respecto.

1.1.11. Análisis y gestión de riesgos

La organización asume el compromiso de controlar los riesgos de seguridad, así como dar cumplimiento a la legislación y normas internas vigente bajo un proceso de mejora continua conforme a los marcos y metodologías existentes en la actualidad (MAGERIT, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas).

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. Para ello, con el objetivo de conocer el nivel de exposición de los activos de información a los riesgos y amenazas en materia de seguridad, los Responsables de Información y de Servicios realizarán análisis de riesgos cuyas consecuencias se plasmarán en actuaciones para tratar y mitigar el riesgo, o incluso, replantear la seguridad de los sistemas en caso necesario.

Se realizará un análisis de riesgos:

- Regularmente, una vez al año.
- cuando haya cambios en los servicios esenciales prestados o cambios significativos en las infraestructuras que los soportan.
- cuando ocurra un incidente de seguridad grave.
- 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.

Las conclusiones de los análisis de riesgos serán elevadas al Responsable de Seguridad y éste al Comité de Seguridad.

Los responsables de la información y/o servicios son responsables de los riesgos sobre la información y/o los servicios 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. Se entiende por Riesgo Residual el riesgo remanente que existe después de que se hayan tomado las medidas de seguridad.

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

La selección de las medidas de seguridad a aplicar será propuesta por el Comité Técnico de Seguridad al Comité de Seguridad Interior y Seguridad TIC, así como el seguimiento de su aplicación.

1.1.12. Gestión de incidentes de seguridad y de la continuidad.

La Consejería de Salud y Familias y sus entidades incluidas en el ámbito de aplicación de la presente Política de Seguridad TIC, deberán estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, según los términos previstos en el artículo 7 del ENS.

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.

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

1.1.13. Instrumentos de desarrollo y estructura normativa

La documentación relativa a la Seguridad de la Información estará clasificada en cuatro niveles, de manera que cada documento de un nivel se fundamenta en los de nivel superior:

- Primer nivel: Política de Seguridad de la Información.
- Segundo nivel: Normativas y Procedimientos de Seguridad.
- Tercer nivel: Procedimientos Técnicos de Seguridad.
- Cuarto nivel: Informes, registros y evidencias electrónicas.

El Comité de Seguridad Interior y Seguridad TIC 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 Política.

11.1. Primer nivel: Política de Seguridad Interior y directrices y normas generales de seguridad TIC.

Documentos de obligado cumplimiento por todo el personal, interno y externo, de la organización, recogido en el presente documento y aprobado mediante Decreto de la organización.

11.2. Segundo Nivel: Normativas de Seguridad

Normas Específicas de Seguridad TIC, que desarrollan y detallan la Política de Seguridad TIC, centrándose en un área o aspecto determinado. De obligado cumplimiento de acuerdo al ámbito organizativo, técnico o legal correspondiente.

La responsabilidad de aprobación de los documentos redactados en este nivel será competencia del Responsable de Seguridad bajo la supervisión del Comité de Seguridad.

11.3. Tercer Nivel: Procedimientos de Seguridad

Procedimientos, Procesos, Guías e Instrucciones Técnicas de Seguridad TIC, que dan respuesta, incluyendo detalles de implementación y tecnológicos, a cómo se puede realizar una determinada tarea cumpliendo con lo expuesto en la Política. Documentos técnicos orientados a resolver las tareas, consideradas críticas por el perjuicio que causaría una actuación inadecuada, de seguridad, desarrollo, mantenimiento y explotación de los sistemas de información.

La responsabilidad de aprobación de estos procedimientos técnicos es del responsable del Sistema de Información correspondiente, bajo la supervisión del Responsable de Seguridad. En caso de que los procedimientos afectaran a varios sistemas de información será responsabilidad del Responsable de Seguridad el aprobarlos.

11.4. Cuarto Nivel: Informes, registros y evidencias electrónicas

Documentos de carácter técnico que recogen el resultado y las conclusiones de un estudio o una valoración; documentos de carácter técnico que recogen amenazas y vulnerabilidades de los sistemas de información, así como también evidencias electrónicas generadas durante todas las fases del ciclo de vida del sistema de información.

La responsabilidad de que existan este tipo de documentos es de cada uno de los responsables de los Sistemas de Información en su ámbito.

11.5. Otra documentación

Se podrá seguir en todo momento los procedimientos, normas e instrucciones técnicas STIC, así como las guías CCN-STIC de las series 400, 500 y 600.

1.1.14. Seguridad de la información

Se desarrollará una Clasificación de la Información de FPS de forma que se identifiquen los distintos tipos de información, en base a su sensibilidad, se establezca cómo etiquetar los soportes que la contengan y se determine qué se puede y no se debe hacer con cada nivel de clasificación.

1.1.15. Obligaciones del personal

Todos los miembros de la organización y las empresas y personas terceras que realicen servicios de cualquier clase contratados por FPS o que de alguna manera se presten bajo el control y/o la dirección de FPS tienen la obligación de conocer y cumplir esta Política de Seguridad y el Cuerpo Normativo de Seguridad. FPS es responsable de comunicar la política y las normas, así como de disponer de los medios necesarios para que todo el personal las conozca de forma efectiva, en especial, las que puedan afectar a sus funciones.

Se establecerá un programa de concienciación continúa dirigido a todos los miembros de FPS, en particular a los de nueva incorporación.

El personal deberá usar los procedimientos de notificación de incidentes de seguridad habilitados a tal efecto, en caso de detectar un posible incidente.

Las personas con responsabilidad en el uso, operación o administración de sistemas de información recibirán formación para el manejo seguro de los sistemas.

1.1.16. Terceras partes

Cuando FPS preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad, se establecerán canales para el reporte y coordinación de los respectivos Delegados de Protección de Datos y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando FPS utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte deberá aceptar el quedar 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 está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política de Seguridad.

Cuando algún aspecto de la Política de Seguridad no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad de la Información 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, así como del responsable del tratamiento previsto en el RGPD, antes de seguir adelante.

1.1.17. Publicación de la política de seguridad

El presente documento se publicará en la sede electrónica de FPS.

1.1.18. Entrada en vigor

La Política de Seguridad Interior que se aprueba será aplicable a partir del día siguiente de su firma y publicación.

Firmado:
Gonzalo Balbontín Casillas
Dirección Gerencia. Fundación Pública Andaluza Progreso y Salud