# Política de Seguridad de la Información

JULIO 2022

Museo CarmenThyssen Málaga

## HISTORIAL DE CAMBIOS

| Nombre del fichero | Versión | Resumen de cambios producidos | Fecha |
|---|---|---|---|
| THYSSEN - STIC 01.01 - Política de Seguridad | 0.00 | Versión borrador | 07/2022 |
| THYSSEN - STIC 01.01 - Política de Seguridad | 1.00 | Versión firmada | 07/2022 |
| | | | |

## CLASIFICACIÓN

| |
|---|
| **INFORMACIÓN PÚBLICA** |
| Nota de confidencialidad: La información contenida en este documento es INFORMACIÓN PÚBLICA.<br><br>Es responsabilidad del Área o Departamento receptor de este documento su distribución interna con base en la necesidad de conocer la información aquí contenida. |

## CONTROL DE DIFUSIÓN

| |
|---|
| AUTOR: Ingenia Babel Cibersecurity |
| DISTRIBUCIÓN:<br>**Fundación Palacio Villalón** |

# Índice

# 1 Introducción

La Fundación Palacio Villalón (en adelante, la Fundación), como muestra de compromiso con la seguridad de la información de sus sistemas[1], 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 (en adelante, ENS), teniendo en cuenta, asimismo, los principios básicos que permiten garantizar el cumplimiento de la legislación en materia de protección de datos vigente, acorde con 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) (en adelante, RGPD) así como la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos de Carácter Personal y garantía de los derechos digitales (en adelante, LOPDgdd).

La Política de Seguridad es una declaración ética, responsable y de estricto cumplimiento de la Fundación, la cual es desplegada a través de las diferentes normas 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 Sistema de información: Conjunto de aplicaciones software, datos, plataformas, equipamiento, locales, personal y otro tipo de elementos que permiten alojar, tratar y administrar información por parte de usuarios para la consecución de un fin.

# 2 Objetivo y ámbito de aplicación

Este documento constituye el establecimiento de una estructura organizativa en materia de seguridad de la información para definirla, implantarla y gestionarla.

Se entenderá la seguridad de la información, 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.

El ámbito de aplicación del presente documento aplica a todos los sistemas de información gestionados por la Fundación.

Afectará a la información tratada por medios electrónicos y a la información en soporte papel que la Fundación gestiona en el ámbito de sus competencias.

Debe ser conocida y cumplida por todas las personas que forman parte de la Fundación, independientemente de cuál sea el vínculo contractual, posición, puesto, cargo y responsabilidad que desempeñen dentro de la organización.

# 3 Normativa de referencia

El marco legal de referencia de las actividades de la Fundación en el ámbito de esta Política de Seguridad está integrado principalmente por los siguientes cuerpos normativos:

- 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.
- 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.
- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, que transpone al ordenamiento jurídico español la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.

# 4 Principios y directrices

Los principios que deben contemplarse en la gestión a la hora de garantizar la seguridad de la información son: prevención, detección, respuesta y recuperación.

Con la observancia de estos principios de actuación se pretende que las amenazas existentes no se materialicen o, en caso de materializarse, no afecten gravemente a la información que maneja o los servicios que presta la Fundación.

## 4.1 Prevención

Se debe 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 deberán implementarse las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos.

Estas medidas y controles, así como los roles y responsabilidades de seguridad de todo el personal de la organización, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la Política de Seguridad se debe:

- 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.

## 4.2 Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple ralentización hasta su detención, se debe 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, en cualquier caso, cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

## 4.3 Respuesta

Se deben llevar a efecto las siguientes actuaciones:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un 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).

### 4.4 Recuperación

Para garantizar la disponibilidad de los servicios críticos, se deben desarrollar planes de continuidad de los sistemas TIC y actividades de recuperación.

Los sistemas dispondrán de copias de seguridad y establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo.

### 4.5 Otros principios generales

- El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado.
- La información debe ser protegida contra accesos y alteraciones no autorizados, manteniéndola confidencial e íntegra.
- Los datos personales serán tratados de tal manera que se garantice una seguridad adecuada de los mismos, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.
- La información debe estar disponible, permitiendo su acceso autorizado, siempre que sea necesario.
- La seguridad de la información es responsabilidad de todos. Todas las personas que tienen acceso a la información de la Fundación deben protegerla, por lo que deben estar adecuadamente formadas y concienciadas. En particular, la seguridad de la información debe contar con el compromiso y apoyo de todos los niveles directivos, de forma que pueda estar coordinada e integrada con el resto de las iniciativas estratégicas de la Fundación.
- Todas las personas que de una forma u otra participen en la utilización, operación, administración o gestión de un sistema de información serán responsables de observar las normas de seguridad establecidas.
- La seguridad de la información no es algo estático, debe ser constantemente controlada y periódicamente revisada.
- Todos aquellos activos (infraestructura, soportes, sistemas, comunicaciones, etc.) donde reside la información, viaja o es procesada, deben estar adecuadamente protegidos.
- Las medidas de seguridad que se implanten deben estar en proporción a la criticidad de la información que protejan y a los daños o pérdidas que se pueden producir en ella. En todo momento se seguirá como mínimo las medidas de seguridad impuestas

por el ENS, así como las guías CCN-STIC elaboradas por el Centro Criptológico Nacional del Centro Nacional de Inteligencia.

- 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. Además, la Fundación exigirá, de manera objetiva y no discriminatoria, que las organizaciones que les presten servicios de seguridad cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados.
- Los sistemas se instalarán en áreas separadas, dotadas de un procedimiento de control de acceso. Como mínimo, las salas deben estar cerradas y disponer de un control de llaves.
- Los sistemas deben diseñarse y configurarse de forma que se garantice la seguridad por defecto tal y como se exige en el artículo 20 del ENS.
- El tratamiento de datos de carácter personal debe estar siempre de acuerdo con las leyes aplicables en cada momento, siendo especialmente importantes:

    - 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).

# 5 Organización de la seguridad de la información

La estructura organizativa de la gestión de la seguridad en el ámbito de la seguridad de la información de la Fundación está compuesta por los siguientes agentes:

- El Comité de Seguridad de la Información (en adelante, también, Comité de Seguridad).
- El Responsable de Seguridad de la Información.
- Los Responsables de la Información y de los Servicios (en adelante, también, Responsables de la Información).
- El Responsable de Sistemas de Información (en adelante, también, Responsable de Sistemas).

## 5.1 Comité de Seguridad de la Información

Para la gestión de la Seguridad de la Información, se crea el Comité de la Seguridad de la Información, en adelante el Comité de Seguridad, dentro del ámbito de la presente Política de Seguridad formado por un equipo multidisciplinar que coordinará las actividades y controles de seguridad establecidos en la Fundación y que vela por el cumplimiento de la normativa vigente, interna y externa, en materia de protección de datos de carácter personal y seguridad.

Las funciones del Comité de Seguridad tendrán las características de estratégicas, regulatorias y de supervisión que abordan aspectos concretos de la seguridad de la información. Estas funciones son:

a) Alinear e identificar los objetivos en el ámbito de la seguridad de la información con la estrategia de la Fundación.
b) Establecer los criterios de revisión de la Política de Seguridad, así como, en su caso, aprobar sus actualizaciones y modificaciones, ya sea a iniciativa propia o a propuesta de cualquiera de los integrantes de la estructura organizativa de la gestión de la seguridad de la seguridad de la información de la Fundación.
c) Promover y respaldar los planes de acción e iniciativas que garanticen la implantación de la Política de Seguridad en la la Fundación.
d) 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.
e) Aprobar los nombramientos de responsables y responsabilidades en materia de seguridad de la información que la Política de Seguridad reserve a este órgano.
f) Proponer y aprobar, según los casos, las normativas y procedimientos internos que se generen en materia de seguridad de la información, así como impulsar el desarrollo normativo que se defina en la Fundación para dar cumplimiento a la Política de Seguridad, según ésta dispone en su apartado 10 (Estructura de la normativa interna), debiendo mantener la documentación organizada y actualizada y gestionar los mecanismos de publicidad y acceso a la misma.
g) Aceptar los riesgos calculados en el análisis de riesgos y realizar su seguimiento y control.

h) Verificar que todas las acciones llevadas a cabo en materia de seguridad de la información sean compatibles o se encuentren respaldadas por la Política de Seguridad.
i) Promover la realización de auditorías periódicas que permitan verificar el cumplimiento de las obligaciones de la Fundación en materia de seguridad.
j) Promover la formación y concienciación en materia de seguridad de la información a todo el personal.
k) Valorar y evaluar los recursos necesarios para dar soporte al proceso de planificación e implantación de la seguridad de la Fundación.
l) Resolver los conflictos que puedan aparecer entre las diferentes personas responsables o entre diferentes áreas de la organización en materia de seguridad de la información.
m) Evaluar de forma periódica el grado de exposición a riesgos que afecten a los sistemas de información, así como evaluar el impacto sobre la protección de datos.
n) Acordar y aprobar metodologías y procesos específicos relativos a la seguridad de la información.
o) Diseñar y ejecutar los programas de actuación propios de la Fundación, incluyendo, entre otros, el Plan de Mejora de la Seguridad, los proyectos de desarrollo normativo y las auditorías de cumplimiento y planes de adecuación legal.
p) 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 Fundación.

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

- Gerencia.
- Los máximos responsables de cada uno de los Departamentos o unidades organizativas del organigrama de la Fundación, pudiendo coincidir esto con los responsables de la información y servicios designados.
- El Responsable de Seguridad de la Información.

Para la celebración de las reuniones del Comité de Seguridad será preciso la presencia de, al menos, el 51% de los miembros permanentes.

El Comité de Seguridad celebrará cuantas reuniones sean necesarias para cumplir sus funciones y, al menos, una vez cada año natural. Estas reuniones tendrán lugar, con carácter general, en la sede de la Fundación, pudiendo designarse otro lugar si así se estima oportuno en cada convocatoria.

La convocatoria de reunión corresponde al Responsable de Seguridad de la Información tanto por iniciativa propia como a instancia de cualquiera de los miembros del Comité.

El Comité de Seguridad adoptará sus acuerdos por mayoría simple de votos.

Se levantará acta de cada una de las sesiones del Comité de Seguridad.

### 5.2 Responsable de Seguridad de la Información

Es el responsable de que los servicios y sistemas de información de la Fundación 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 proporcionados por la Fundación permanecerán disponibles.

Son funciones del Responsable de Seguridad de la Información:

a) Supervisar el cumplimiento de la presente Política, normativas y procedimientos derivados de la misma.
b) Asesorar en materia de seguridad a los integrantes de la Fundación 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) Establecer las medidas de seguridad, adecuadas y eficaces, para cumplir los requisitos de seguridad establecidos por los Responsables de la Información, siguiendo en todo momento lo exigido en el Anexo II del ENS.
f) Asesorar, en colaboración con el Responsable de Sistemas y los Responsables de la Información, en la realización de los análisis y gestión de riesgos, elevando el informe resultante 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 y, en su caso, realizar las convocatorias para las reuniones del mismo.
i) Proponer 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 el Responsable de Sistemas antes de ser ejecutada.
j) Elevar al Comité de Seguridad las actuaciones para tratar y mitigar el riesgo derivadas del análisis de riesgos previsto en el apartado 9 de esta Política.
k) Proponer y aprobar, según los casos, las normativas y procedimientos internos que se generen en materia de seguridad de la información, así como impulsar el desarrollo normativo que se defina en la Fundación para dar cumplimiento a la Política de Seguridad, según ésta dispone en su apartado 10 (Estructura de la normativa interna), debiendo mantener la documentación organizada y actualizada y gestionar los mecanismos de publicidad y acceso a la misma.

El Responsable de Seguridad de la Información es la figura que determina las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos.

El Responsable de Seguridad de la Información será nombrado y cesado por la Gerencia de la Fundación.

### 5.3 Responsables de la Información y de los Servicios

Los **Responsables de la Información y de los Servicios** serán quienes en primera instancia determinen la finalidad, contenido y uso de la información que se genera y gestiona dentro de su marco de competencias. Las principales funciones, dentro de su ámbito de actuación, son las siguientes:

a) Ayudar a determinar los requisitos de seguridad de la información, clasificando la información conforme a los criterios y categorías establecidas en el ENS y en cada una de las dimensiones de seguridad conocidas y aplicables (disponibilidad, autenticidad, trazabilidad, confidencialidad e integridad), dentro del marco establecido en el Anexo I del ENS.
b) Proporcionar la información necesaria al Responsable de Seguridad de la Información para realizar los preceptivos análisis de riesgos, con la finalidad de establecer las salvaguardas a implantar. Para ello contará con la ayuda del Responsable de Sistemas.
c) Verificar que los análisis de riesgos realizados se corresponden en todo momento con la información aportada para la realización de los mismos.
d) Colaborar en la evaluación de los riesgos residuales calculados en el análisis de riesgos y realizar su seguimiento y control.
e) Colaborar con el Responsable de Seguridad de la Información proporcionando la información necesaria acerca del tratamiento de datos personales que se lleve a cabo en el servicio.
f) Velar por el cumplimiento de la normativa de seguridad y protección de datos personales definida por la organización en el servicio.
g) Proponer 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 Seguridad de la Información y el Responsable de Sistemas antes de ser ejecutada.
h) Ejecutar los requisitos de seguridad organizativos, técnicos y de control que deben cumplir los sistemas y servicios de la Fundación.
i) Informar y asesorar al Comité de Seguridad y asistir a las reuniones del mismo cuando sea convocado.
j) Realizar, junto con el Responsable de Sistemas, análisis de riesgos de acuerdo con lo previsto en el apartado 9 de esta Política, cuyas consecuencias se plasmarán en actuaciones para tratar y mitigar el riesgo y serán elevadas al Responsable de Seguridad de la Información.

Los Responsables de la Información son nombrados y cesados por el Comité de Seguridad a propuesta de los máximos responsables de cada Departamento o Área.

### 5.4 Responsable de Sistemas

Es la persona designada a los efectos de dar cumplimiento a esta Política cuyas responsabilidades sobre todos los sistemas de información existentes en la organización son las siguientes:

a) Realizar el desarrollo, operación y mantenimiento de los sistemas de información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
b) Garantizar que las medidas de seguridad se integren adecuadamente dentro del marco general de la seguridad de la información.
c) Informar sobre toda modificación sustancial de la configuración de cualquier elemento del sistema.
d) Elaborar procedimientos de seguridad de los sistemas de información.
e) Elaborar Planes de Continuidad de los sistemas de información, si procede.
f) Informar y asesorar al Comité de Seguridad y asistir a las reuniones del mismo cuando sea convocado.
g) Proponer 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 el Responsable de Seguridad de la Información antes de ser ejecutada.
h) Promover las medidas que el apartado 4.1 de esta Política establece para garantizar el cumplimiento de la Política de Seguridad con relación al principio de prevención.
i) Realizar, junto con los Responsables de la Información, análisis de riesgos de acuerdo con lo previsto en el apartado 9 de esta Política, cuyas consecuencias se plasmarán en actuaciones para tratar y mitigar el riesgo y serán elevadas al Responsable de Seguridad de la Información.

El Responsable de Sistemas es nombrado y cesado por el Comité de Seguridad a propuesta del máximo responsable del Departamento o Área al que esté adscrita el área de Sistemas de Información (TIC´s).

### 5.5 Resolución de conflictos

En caso de conflicto entre los diferentes responsables definidos en la política, éste será resuelto por el superior jerárquico de los mismos. En defecto de lo anterior, prevalecerá la decisión del Comité de Seguridad.

### 5.6 Obligaciones del personal

Todo el personal, interno o externo, de la Fundación 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.

Asimismo, deberá cumplir además con las instrucciones y normas que regulen el comportamiento del personal en el uso de los sistemas informáticos y redes de comunicaciones de la Fundación.

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.

# 6 Asesoramiento especializado en materia de seguridad

## 6.1 Asesoramiento especializado

El Responsable de Seguridad de la Información será el encargado de coordinar los conocimientos y las experiencias disponibles en la Fundación 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, la Fundación mantendrá contactos periódicos con organismos y entidades especializadas en temas de seguridad tales como:

- CCN-CERT: Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional (CCN), dependiente del Centro Nacional de Inteligencia (CNI), como soporte y coordinación para la resolución de incidentes que sufra la Administración General, Autonómica o Local.
- Agencia Española de Protección de Datos (AEPD): velando por el cumplimiento de la legislación sobre protección de datos de carácter personal y controlando su aplicación.
- Instituto Nacional de Ciberseguridad (INCIBE) – CERT Centro de Respuesta a Incidentes de Seguridad: ofreciendo soluciones reactivas a incidentes informáticos, servicios de prevención frente a posibles amenazas y servicios de información, concienciación y formación en materia de seguridad (www.incibe.es)
- Grupo de Delitos Informativos Informáticos y Telemáticos de la Guardia Civil y Brigada de Investigación Tecnológica (BIT) del Cuerpo Nacional de Policía: investigando acciones relacionadas con la delincuencia informática y los fraudes en el sector de las telecomunicaciones que le encomienden las Autoridades Judiciales o que conozca por comunicaciones y denuncias de los ciudadanos y que por su importancia o relevancia social, dificultad técnica o número de afectados, aconseje la dedicación de este grupo.

## 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 de la Fundación reflejan adecuadamente sus disposiciones.

# 7 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 las políticas de protección de datos internas y de acuerdo 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), así como lo establecido en la Ley 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de derechos digitales (LOPDgdd).

# 8 Formación y concienciación

El objetivo es lograr la plena conciencia respecto a que la seguridad de la información que afecta a todo el personal de la Fundación y a todas las actividades de acuerdo al principio de seguridad integral recogido en el art. 5 y 6 del ENS. A estos efectos, la Fundación propondrá y organizará sesiones informativas, 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 y puedan acceder a dicha información.

# 9 Análisis y gestión de riesgos

La Fundación asume el compromiso de controlar los riesgos de seguridad, así como dar cumplimiento a la legislación y normas internas vigentes bajo un proceso de mejora continua conforme a los marcos y metodologías existentes en la actualidad.

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, el Responsable de Sistemas, junto con los Responsables de la Información, realizará, con periodicidad al menos anual, un 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, al menos 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 de la Información, y éste lo trasladará al Comité de Seguridad.

# 10 Estructura de la normativa interna

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:

| Niveles | Documentos | Responsables |
|---|---|---|
| Primer | Política de Seguridad de la Información | Gerencia |
| Segundo | Normativas de Seguridad | Comité de Seguridad |
| Tercero | Procedimientos de Seguridad | Responsable de Seguridad de la Información |
| Cuarto | Informes, registros y evidencias electrónicas | Responsable de Sistemas |

## 10.1 Primer nivel: Política de Seguridad de la Información

Política de obligado cumplimiento por todo el personal, interno o externo, de la Fundación que se recoge en el presente documento, siendo aprobada por acuerdo de Gerencia.

Sus modificaciones podrán ser aprobadas por el Comité de Seguridad, quien dará cuenta de ello a la Gerencia y dirección de la Fundación.

## 10.2 Segundo Nivel: Normativas de Seguridad

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 Comité de Seguridad, a propuesta del Responsable de Seguridad de la Información.

## 10.3 Tercer Nivel: Procedimientos de Seguridad

Documentos 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 es del Responsable de Seguridad de la Información, ya sea a iniciativa propia o ya sea a propuesta del Responsable de Sistemas.

### 10.4 Cuarto Nivel: Informes, registros y evidencias electrónicas

Se incluyen en este nivel los documentos de carácter técnico mediante los que el Responsable de Sistemas recoge el resultado y las conclusiones de un estudio o una valoración y los documentos de carácter técnico que recogen amenazas y vulnerabilidades de los sistemas de información, así como también las evidencias electrónicas generadas durante todas las fases del ciclo de vida del sistema de información.

La responsabilidad de que exista este tipo de documentos es de cada uno de los Responsables de la Información en su ámbito.

### 10.5 Otra documentación

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

## 11 Publicación de la Política de Seguridad

La presente Política será publicada en la página web de la Fundación.

25062766B
FRANCISCO
JAVIER FERRER
(R: G93003150)

Firmado digitalmente por 25062766B FRANCISCO JAVIER FERRER (R: G93003150)
Nombre de reconocimiento (DN): 2.5.4.13=Ref:AEAT/AEAT0446/PUESTO 1/19025/29042021112605, serialNumber=IDCES-25062766B, givenName=FRANCISCO JAVIER, sn=FERRER MORATO, cn=25062766B FRANCISCO JAVIER FERRER (R: G93003150), 2.5.4.97=VATES-G93003150, o=FUNDACION PALACIO VILLALON, c=ES
Fecha: 2022.07.22 13:49:25 +02'00'

# 12 Entrada en vigor

La Política de Seguridad será aplicable a partir del día siguiente de la fecha de su aprobación.

Málaga, 15 de julio de 2022