Política de seguridad de la información

HISTORIAL DE CAMBIOS

Nombre del fichero	Versión	Resumen de cambios producidos	Fecha
Política de seguridad de la información	1.00	Primera versión.	30/11/2024
Política de seguridad de la información	2.00	Segunda versión	27/01/2026
Política de seguridad de la información	2.01	Segunda versión corregida	23/04/2026

CLASIFICACIÓN

USO INTERNO
La información contenida en este documento es USO INTERNO.

CONTROL DE DIFUSIÓN

AUTORÍA: Fundación Española para la Ciencia y la Tecnología, F.S.P.
DISTRIBUCIÓN: Fundación Española para la Ciencia y la Tecnología, F.S.P.

REFERENCIAS

Contenido

1. INTRODUCCIÓN 5
2. MISIÓN DE LA FECYT 6
3. PRINCIPIOS RECTORES DE LA POLÍTICA 7
4. ALCANCE 8
5. MARCO NORMATIVO 9
6. ORGANIZACIÓN DE LA SEGURIDAD 9
6.1. Principios de la gobernanza 9
6.2. Estructura de la gobernanza 10
6.2.1. Estructura de gobierno 11
6.2.1.1. Comité de Seguridad de la Información 11
6.2.1.2. Responsable de la información y transformación digital 14
6.2.1.3. Responsable de los Servicios 15
6.2.2. Estructura de supervisión 16
6.2.2.1. Presidencia 16
6.2.2.2. Responsable de Seguridad de la Información 16
6.2.3. Estructura de operación 17
6.2.3.1. Responsable del Sistema 18
6.2.3.2. Responsable de Infraestructura IT 18
6.2.3.3. Responsable de la Seguridad Física 19
6.2.3.4. Personas usuarias de los sistemas 20
6.2.4. Otros roles 20
6.2.4.1. Administradores de seguridad 20
6.2.4.2. Persona delegada de Protección de Datos (DPD) 20
6.2.5. Servicios de Soporte 21
6.3. Reportes entre los diferentes roles y responsables 22
7. FUNCIONES Y OBLIGACIONES 22
7.1. Funciones y obligaciones de terceras partes 22
7.2. Resolución de conflictos 23
8. FORMACIÓN Y CONCIENCIACIÓN 23

9. GESTIÓN DE RIESGOS 23

10. DATOS DE CARÁCTER PERSONAL 24

11. GESTIÓN DE INCIDENTES DE SEGURIDAD 25

12. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 26

12.1. Estructura normativa 26

13. INCUMPLIMIENTO 27

14. REVISIÓN Y APROBACIÓN 27

ANEXO I. MARCO NORMATIVO 29

ANEXO II. GLOSARIO 31

1. INTRODUCCIÓN

En el ecosistema en el que nos movemos, se ha digitalizado y ha empezado a requerir del uso de las tecnologías y de los nuevos componentes que han irrumpido con fuerza para facilitar gran parte de nuestras actividades diarias. Sin duda la revolución en la que nos encontramos facilita y simplifica muchas tareas, y nos agiliza plazos que en muchas ocasiones se volvían tediosos, pero también conllevan desventajas y riesgos que no pueden ser ignorados.

Las nuevas [ciber]amenazas, vienen de la mano de nuevos actores maliciosos que persiguen el mayor impacto en sus potenciales ataques, con mayores frecuencias de ataque, habilidades mejoradas y una clara intencionalidad, causar el mayor daño posible.

Y las entidades del sector público hemos pasado a ser un objetivo prioritario en la escena de ciber amenazas, convirtiendo la seguridad de la información en un elemento prioritario de nuestra estrategia anual, con el impulso de los cambios legislativos que nos rodean y con la alianza estratégica del sector privado.

Los nuevos desafíos y riesgos que se nos presentan requieren respuestas adaptadas, coordinadas e innovadoras que permitan desplegar una estrategia completa, proactiva y que garantice la continuidad y resiliencia de nuestros servicios, sobre la protección de las infraestructuras tecnológicas y de la información digital que requerimos para nuestro normal funcionamiento y prestar adecuadamente los servicios a la ciudadanía. De aquí, necesariamente se deriva la priorización y apoyo de la seguridad de las tecnologías de la información, la ciberseguridad con especial atención al ámbito de la protección de las redes y sistemas de información que utiliza la ciudadanía en su normal desenvolvimiento con la fundación, las empresas y el resto de las entidades públicas.

Por todo ello, la Fundación Española para la Ciencia y la Tecnología, F.S.P. (en adelante, FECYT) como Fundación del sector público estatal, conforme a lo previsto en la Ley 50/2002, de Fundaciones y en la Ley 47/2003, General Presupuestaria, ha considerado necesario desplegar una estrategia de alto nivel, que se acomoda a los mandatos normativos, respetando plenamente la voluntad del fundador manifestada en sus Estatutos y las disposiciones establecidas por el Patronato. Esta estrategia se materializa con la presente Política de Seguridad de la Información de la FECYT, en cumplimiento del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, en adelante ENS, relativo a los requisitos mínimos de Seguridad en el ámbito de la Administración Electrónica.

Y en base a lo anterior, esta política implica asumir los siguientes **objetivos estratégicos** de seguridad de la información:

- La política de seguridad se encuentra alineada con el marco normativo y el contexto estratégico perteneciente al ENS para garantizar la seguridad en la Administración Digital.
- Mantener el pleno cumplimiento de la normativa vigente en privacidad y protección de datos, de manera que se mantenga el correcto tratamiento de los datos

personales implicados.

- Mantener la conformidad con el Esquema Nacional de Seguridad, adoptando todas las medidas precisas para el cumplimiento, bajo los criterios aprobados por la Autoridad de Control.
- La Política de Seguridad de la Información recoge la postura de la FECYT en cuanto a la seguridad de la información y establece que ente los criterios generales que deben regir la actividad del organismo, se encuentra la seguridad por defecto y desde el diseño.
- Promover acciones de formación y concienciación en seguridad de la información y, garantizar la difusión de esta Política.
- 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.

La FECYT se compromete a la mejora continua de la seguridad de la información, mediante la revisión periódica de su adecuación, eficacia y alineación con los riesgos identificados, el marco normativo aplicable y los objetivos de la Fundación.

Los sistemas de información deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad, uso previsto y valor de la información y los servicios.

La actualización de esta política responde a la necesidad de optimizar su funcionamiento y adecuarla a los cambios normativos, tecnológicos y organizativos que se han producido desde su versión anterior. La experiencia en su aplicación ha evidenciado áreas que requieren mayor claridad y actualización para garantizar una gestión de la seguridad más eficaz y alineada con las necesidades actuales de la FECYT.

2. MISIÓN DE LA FECYT

La FECYT es una fundación del sector público estatal dependiente del Ministerio de Ciencia, Innovación y Universidades.

Su fin fundacional es fomentar el compromiso de la sociedad con la ciencia, la tecnología y la innovación como valor clave para su desarrollo y bienestar mediante acciones que promuevan la ciencia abierta e inclusiva, la cultura y la educación científicas, dando respuesta a las necesidades y retos del sistema español de ciencia, tecnología e innovación, facilitando herramientas y recursos que contribuyan a la internacionalización de la ciencia y la competitividad de la industria.

La FECYT es el principal impulsor y organismo vertebrador del fomento de la cultura científica en España, en línea con el Plan Estatal de Investigación Científica, Técnica y de Innovación 2024-2027 y la Ley 14/2011 de 1 de junio de la Ciencia, la Tecnología y la Innovación. La estrecha situación de los recursos humanos disponibles exige el establecimiento claro de prioridades en una programación ajustada y eficaz.

La actividad principal de la FECYT se desarrolla desde el edificio del Museo Nacional de

Ciencia y Tecnología, en la calle Pintor Murillo número 15 de Alcobendas. Una pequeña parte de su personal realiza su actividad en la sede de A Coruña del museo, en la plaza Museo Nacional de Ciencia, número 1.

La FECYT mantiene un compromiso prioritario con la Seguridad de la Información para toda la organización, a la vez que quiere satisfacer determinadas necesidades de los agentes del Sistema Español de Ciencia, Tecnología e Innovación.

3. PRINCIPIOS RECTORES DE LA POLÍTICA

El objeto de la presente Política es establecer la postura de la FECYT respecto a la Seguridad que afecta a los procesos relacionados con el desenvolvimiento de su actividad y, muy particularmente, con los relacionados con la administración electrónica, tanto desde el punto de vista de las personas usuarias de los servicios, como desde el punto de vista interno, para la gestión de la propia Entidad.

La FECYT utiliza las Tecnologías de la Información y las Comunicaciones para prestar sus servicios, por lo que es consciente de que estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la seguridad de la información tratada o los servicios prestados.

Asimismo, también es consciente de que los incidentes de seguridad pueden estar provocados desde lugares remotos, a través de las conexiones a redes de comunicaciones de las que se dispone y, muy concretamente, a través de las conexiones a Internet (ciberataques), y que estos pueden suponer una potencial amenaza para la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información tratada y de los servicios prestados.

La política de la FECYT es la de contrarrestar las amenazas mencionadas anteriormente con los medios suficientes, teniendo en cuenta su disponibilidad presupuestaria. Para este fin, se establecerá una estructura de seguridad, junto con los mecanismos apropiados para su gestión, y un conjunto de instrumentos de apoyo de forma que se garantice:

- el cumplimiento de los objetivos de su misión y de prestación de servicios.
- el cumplimiento de la legislación y normativa aplicables.

Para ello,

- se preverán y desplegarán medidas para evitar incidentes de seguridad que pudieran afectar al cumplimiento de objetivos o poner en riesgo la información.
- se diseñarán medidas de respuesta ante incidentes de seguridad, física o lógica, de forma que se minimice el impacto de estos, en caso de que ocurrieran.

Como norma general, el análisis de riesgos será la base a la hora de diseñar las medidas de seguridad necesarias, poniendo más foco y esfuerzo en la mitigación de lo que suponga un mayor riesgo.

Las distintas áreas bajo cuya responsabilidad se encuentran los servicios prestados deberán contemplar la seguridad desde el mismo momento en que se concibe un nuevo sistema o servicio, aplicando para estos y para los ya existentes, las medidas de seguridad prescritas por el ENS para garantizar la disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad de los servicios y de la información.

Los requisitos de seguridad de los sistemas, las necesidades de formación de las personas usuarias, administradores y operadores y las necesidades de financiación deben ser identificados e incluidos en la planificación de los sistemas y en los pliegos de prescripciones utilizados para la realización de proyectos que involucren a las TIC.

Se deben articular mecanismos de prevención, reacción y recuperación con objeto de minimizar el impacto de los incidentes de seguridad.

En cuanto a la **prevención**, se debe evitar que los servicios y la información resulten afectados por un incidente de seguridad. Para ello, la FECYT implementará las medidas de seguridad establecidas en el Anexo II del ENS, así como aquellas medidas adicionales que pudieran ser identificadas en el proceso de análisis de riesgos.

En cuanto a la **reacción**, se establecerán mecanismos de detección, comunicación y gestión de incidentes de seguridad, de forma que cualquier incidente pueda ser tratado en el menor plazo posible. Siempre que sea posible, se detectarán de forma automática los incidentes de seguridad, utilizando elementos de monitorización de los servicios o de detección de anomalías y poniendo en marcha los procedimientos de respuesta al incidente en el menor plazo posible. Para los incidentes detectados por las personas usuarias, ya sean internos o externos, se establecerán los pertinentes canales de comunicación de incidentes.

En cuanto a la **recuperación**, para aquellos servicios que se consideren críticos, en base a la valoración que de los mismos realicen sus responsables, se deberán desarrollar planes que permitan la continuidad de dichos servicios en el caso de que, a raíz de un incidente de seguridad, quedaran indisponibles.

4. ALCANCE

La presente se aplica a los sistemas de información que soportan los servicios públicos prestados por la FECYT y que constituyen su Sistema de Información, así como sus subsistemas.

Se incluyen expresamente los sistemas, activos y servicios. En todo caso se ven afectadas las personas prestadoras y las personas usuarias en las que además, reside la obligación de velar por el cumplimiento de ésta.

En relación con las personas usuarias, se consideran todas aquellas con acceso a los sistemas sean o no personal interno de la entidad propietaria de los sistemas y en todo caso, teniendo la obligación de conocer y cumplir con la misma y de cuanta normativa y procesos se desplieguen por mandato de ésta.

5. MARCO NORMATIVO

Esta política se sitúa dentro del marco del marco normativo recogido en el Anexo. También forman parte del marco normativo de seguridad las restantes normas aplicables a la Administración Electrónica.

La FECYT será responsable de identificar las correspondientes guías de seguridad de las tecnologías de la información y la comunicación (guías CCN-STIC), que serán de aplicación para mejorar el cumplimiento de lo establecido en el ENS, y que incluyan las medidas y refuerzos que deben desplegarse, en el sistema de información sometido a esta Política.

6. ORGANIZACIÓN DE LA SEGURIDAD

La organización de la seguridad de los sistemas de información de la FECYT diferencia las responsabilidades necesarias para mantener la segregación de roles y mantener las funciones de seguridad asignadas. Y ello de conformidad con lo establecido en el artículo 11 del ENS. La presente política declara los roles o funciones de seguridad que existirán en la fundación y define para cada uno, sus deberes y responsabilidades, así como el procedimiento para su designación y renovación.

Se detalla la estructura y composición de los órganos colegiados que se encargarán de la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, las funciones, los flujos e interconexiones existentes con otras funciones clave.

La gobernanza de la seguridad de la información de la FECYT se ha considerado sobre la Estrategia de Seguridad de la Información conforme a la normativa vigente, guías de CCN-CERT y prácticas reconocidas en el sector, y que se detalla a continuación.

6.1. Principios de la gobernanza

La gobernanza de la seguridad de la información en la FECYT se enmarca sobre los siguientes principios:

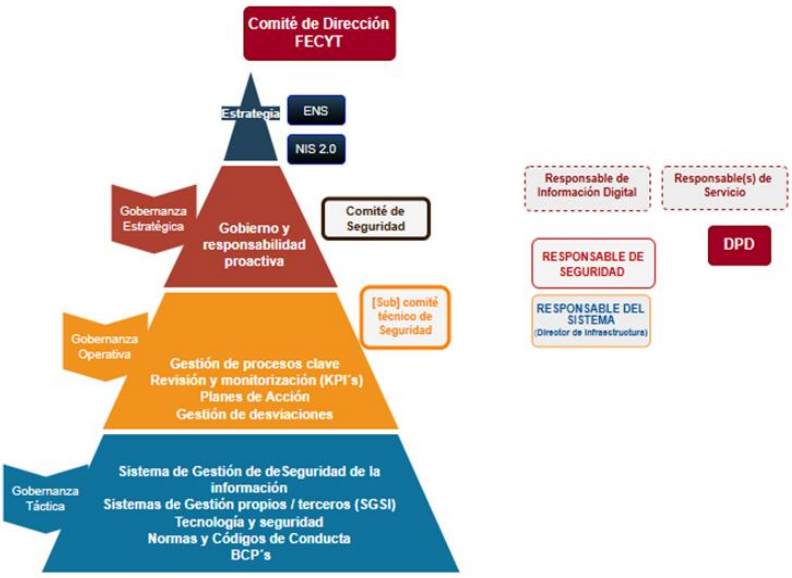
- La gobernanza se presenta como clave para la prevención proactiva de la seguridad y se designarán tantos órganos, unidades, grupos o responsables que sean necesarios para desplegar la seguridad de la información de manera adecuada, robusta y adaptada a la estructura y funciones de la entidad.
- Los roles y responsabilidades de la estructura de gobernanza de la seguridad se ajustarán a los requisitos establecidos en el ENS y normativa aplicable.
- Los órganos existentes en la estructura orgánica actual de la entidad interactuarán con pleno derecho en el marco de gobernanza de la seguridad de la información, recibirán los reportes necesarios en tiempo y forma, y formarán parte de esta cuando se considere que generan las sinergias de seguridad necesarias, con las competencias establecidas y aprobadas por el máximo órgano de seguridad de la información.
- Todas las áreas, departamentos, servicios, unidades, o cualquier estructura que se defina en la organización y en general todas las personas usuarias, quedan sometidas en sus actuaciones, a las instrucciones emanadas de los órganos, roles y

responsables definidos en esta Política.

6.2. Estructura de la gobernanza

Se establecerán las siguientes estructuras:

- Estructura de gobierno, que se encarga de desplegar la estrategia de seguridad de la información y velar por el desarrollo del cumplimiento.
- Estructura de supervisión, que es la que se encarga de verificar el cumplimiento de los requisitos de seguridad y el alineamiento continuo con los objetivos de la organización.
- Estructura de operación, que se encarga de implantar las medidas de seguridad identificadas.



Conforme al ENS, las guías del CCN-CERT y las mejores prácticas de seguridad de la información se definen en la presente los principales **roles y responsabilidades** de seguridad de la información:

a. Responsable(s) de Información y transformación digital.
b. Responsable (s) y Servicio.
c. Responsable(s) de Seguridad.
d. Responsable(s) del Sistema.

Además, se consideran otros roles cuyas responsabilidades se consideran de relevancia para la seguridad de la información:

e. Responsable(s) de Infraestructura.
f. Responsable(s) de Seguridad Física.

Sobre los roles y responsabilidades descritos, se han considerado distintos **órganos colegiados de gobernanza** cuyas funciones diferenciadas permitirán garantizar el despliegue de la estrategia de seguridad de la información:

a. Comité de Seguridad de la Información.

c. [Sub] Comité Técnico de Seguridad de la Información.

Además, se han considerado en la capa estratégica de la seguridad, unos **servicios de soporte** que desarrollarán funciones y actividades de seguridad, tanto de soporte para medidas de técnicas y de gestión de seguridad, medidas de ciberseguridad, operativas de ciberseguridad y monitorización, desarrollo y cuantas otras pudieran ser consideradas.

Los roles serán asumidos por aquellas personas que reúnan los requisitos de capacitación y dispongan de la cualificación que pudieran ser requerida. La designación se hará constar en el acta del comité y se hará efectiva con la comunicación a la persona que ostente el rol, mediante notificación expedida por la Secretaría del comité. Podrá considerarse la asunción de las responsabilidades y por ello roles colegiados, a alguno de los órganos creados al amparo de la presente.

El máximo órgano colegiado de seguridad de la información podrá considerar la designación de nuevos roles de seguridad, a propuesta del responsable de Seguridad y/o responsable del Sistema, y en caso de ser aprobados, constarán en acta hasta la operativa modificación de la presente.

El máximo órgano o aquellos órganos operativos de seguridad podrán considerar la creación de servicios de soporte, unidades o grupos de trabajo para mejorar la seguridad de la información o la mejora en la implantación o mantenimiento de medidas de seguridad.

El responsable de Seguridad y el responsable del Sistema podrán designar Administradores de Seguridad, que serán roles de soporte y ayuda en sus funciones específicas, pero en ningún caso podrán delegarse las responsabilidades.

6.2.1. Estructura de gobierno

Encargada de desplegar la estrategia de seguridad de la información, está compuesta por el máximo órgano de seguridad en la entidad, y del emanarán las directrices de seguridad.

Se considera al Comité de Seguridad de la Información como máximo órgano de seguridad de la FECYT.

6.2.1.1. Comité de Seguridad de la Información

Órgano colegiado, especializado y permanente de la seguridad de la información y está compuesto por las personas con responsabilidad en materia de seguridad, y aquellas que han sido designadas por otros órganos o que son requeridas para mantener la seguridad del sistema.

La misión del Comité de Seguridad es la coordinación general de las actividades que tienen relación con la seguridad integral.

Su funcionamiento se regirá por su propia norma interna o reglamento, donde se regulará las

convocatorias, evidencia de acuerdos, quorum necesario, metodología de desarrollo de sesiones, acceso a información, representaciones, cargos internos, y cualquier otra medida que se considere necesaria. En cualquier caso, las reuniones serán convocadas por su presidencia, a través de la secretaría, a su iniciativa o por mayoría de las personas integrantes permanentes. Las decisiones se adoptarán por mayoría de las personas integrantes permanentes y presentes en la reunión

Un objetivo fundamental del Comité de Seguridad es la puesta en común de aspectos importantes de la seguridad entre todos los responsables. Con ello se evitará que actividades referentes a la seguridad, que puedan afectar a varias o todas las áreas de la organización, queden sin el suficiente conocimiento por parte de sus responsables, o sin el suficiente apoyo o compromiso, perjudicando su eficacia.

Las funciones del Comité de Seguridad son:

- Identificar los objetivos de la FECYT en el ámbito de la Seguridad de la Información, y proponer los objetivos estratégicos de la FECYT en materia de ciberseguridad en el Plan Estratégico, y de la actividad anual en los Planes de Actuación y los objetivos en materia de ciberseguridad valorables para la promoción y/o retribuciones especiales de personal.
- Elaborar la Política de Seguridad, establecer los criterios de revisión de esta, revisarla, distribuirla y velar por su cumplimiento.
- Promover y respaldar los planes de acción e iniciativas que garanticen la implantación de la Política de Seguridad en la FECYT y supervisar su desarrollo.
- Establecer los requisitos de seguridad que deben cumplir a nivel organizativo, técnico y de control, los sistemas y servicios de la FECYT.
- 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.
- Comunicar a los terceros que colaboren en la explotación de los sistemas de información la realización de esta conforme a lo exigido en el ENS.
- Diseñar e implantar los indicadores necesarios para medir la eficacia y eficiencia de las medidas adoptadas. Verificar el correcto funcionamiento de los indicadores de seguridad de la información.
- Definir las especificaciones funcionales de seguridad de los Sistemas de Información de la Organización resultantes del análisis y gestión de riesgos, de la información fruto del análisis de los indicadores implementados, y de las pautas del Anexo II del Esquema Nacional de Seguridad.
- Valorar el grado de conformidad de los procedimientos implantados en la FECYT con las normas definidas en la política, estableciendo planes de mejora para aquellos que requieran de una modificación para su conformidad.
- Aprobar los procedimientos de seguridad que forman parte del Mapa Normativo (y no son competencia del responsable de Seguridad) y tomar conocimiento de las modificaciones de procedimientos que, en su caso, se hayan realizado a lo largo del periodo en curso, y coordinar su presentación al Comité de Dirección.
- Acordar y aprobar metodologías y procesos específicos relativos a la Seguridad de la Información.

- Verificar que todas las acciones llevadas a cabo en materia de seguridad sean compatibles o se encuentren respaldadas por la Política de Seguridad.
- Promover la formación y concienciación en materia de Seguridad de la Información a toda la plantilla.
- Determinar y proponer los requisitos de formación para las personas clave que manejan información, sistemas e infraestructuras físicas y que se integrarán en el Plan Anual de Formación en Ciberseguridad.
- Proponer para su aprobación los planes de mejora de la seguridad que surjan a raíz de los análisis de riesgos realizados.
- Analizar la información de los indicadores de seguridad que pudiera haber definidos y tomar las decisiones que correspondan en caso de desviación respecto a los umbrales establecidos.
- Coordinar las actuaciones en materia de seguridad que se puedan estar realizando en diferentes áreas de la Organización con objeto de evitar esfuerzos duplicados o desalineados con la Política de Seguridad de la Información.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto a ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de tales incidentes.
- Valorar y evaluar los recursos necesarios para dar soporte al proceso de planificación e implantación de la seguridad en la FECYT.
- Resolver los conflictos de responsabilidad que puedan surgir entre los diferentes responsables y/o entre diferentes áreas.

Formarán parte permanente del Comité de Seguridad:

- La Gerencia de la FECYT, que ostentará la Presidencia.
- Responsable de Seguridad de la Información.
- Responsable de Sistema.
- Responsable(s) de la información y transformación digital.
- Responsable(s) del servicio.
- Responsable(s) de Infraestructura IT.
- Responsable(s) de Seguridad Física.

La persona delegada de Protección de Datos (DPD) participará con voz, pero sin voto en las reuniones del Comité de Seguridad de la información cuando en el mismo vayan a abordarse cuestiones relacionadas con el tratamiento de datos de carácter personal, así como siempre que se requiera su participación. En todo caso, si un asunto se sometiese a votación, se hará constar siempre en acta la opinión de la DPD.

Adicionalmente, podrán asistir al Comité de Seguridad los responsables de las materias específicas a tratar en las reuniones, que podrán ser invitados en función del contenido de la agenda.

Una vez alcanzada la Certificación de Conformidad con el ENS de los servicios de la FECYT incluidos en el mismo, el Comité de Seguridad se reunirá, al menos, una vez al año, sin perjuicio de que, en atención a las necesidades derivadas del cumplimiento de sus fines y atribuciones, requiera de una mayor frecuencia de las reuniones.

El Comité de Seguridad, dado su carácter estratégico podrá constituir un Subcomité de seguridad de la información, órgano colegiado, especializado y de carácter técnico y de ciberseguridad. Este asumirá todas las funciones delegadas por el comité y, además;

- Gestionar la ejecución de las medidas de seguridad aprobadas por el Comité de Seguridad de la Información
- Colaborar en la etapa de identificación y valoración de los riesgos, y en la elaboración de propuestas para la mitigación de los riesgos.
- Seguimiento de las vulnerabilidades detectadas en procesos de revisión y de sus planes de acción, y bastionados de sistemas.
- Validar el cierre de la Informe anual de estado de seguridad. (Encuesta INES)
- Gestión de la capacidad y propuestas anuales. Seguimiento del plan.
- Preparación de informe anual sobre el estado de capacidad y la gestión de sus necesidades.
- Estudio y elaboración de propuestas y planes de seguridad para remisión al órgano competente.
- Elaboración de propuestas de formación del personal en materia de seguridad.
- Coordinación en caso de brechas de seguridad o de incidentes de seguridad relevantes.
- Desarrollo y aprobación de procedimientos IT y colaboración en la definición de otros procedimientos e instrucciones de seguridad, de tercer nivel.
- Colaboración en el desarrollo de planes de contingencia.

Las funciones del subcomité requieren que su funcionamiento sea hibrido, es decir operativo y táctico y requerirá sesiones de trabajo con una periodicidad reducida, en modo tanto extraordinarias y urgentes.

El subcomité deberá reunirse al menos una vez al mes, para las funciones ordinarias encomendada, y por medio del responsable(s) del Sistema, mantendrá un flujo permanente con el responsable(s) de Seguridad. Se realizarán reportes periódicos al Comité de Seguridad de la Información.

6.2.1.2. Responsable de la información y transformación digital

La FECYT ha considerado la importancia de la transformación digital en sus procesos y su impacto directo en la seguridad de la información, por lo que el rol de responsable de la información será, además de responsable de las funciones clave de este rol, responsable de las funciones de transformación digital, y garante de la seguridad del dato digital. En este contexto será el rol que asuma funciones de digitalización y transformación, asumiendo el liderazgo en esta materia.

Será un perfil dual que desarrollará sus funciones de manera única y consagrando la seguridad de ambas responsabilidades:

a) Responsable de la Información. Requisitos de seguridad de la información.
b) Responsable de la transformación digital: Requisitos de seguridad del dato digital.

Serán funciones de este perfil:

- Determinar los requisitos de la información tratada.
- Valorar la información, conforme a lo estableció en el Real Decreto 311/2022, instrucciones aplicables, así como las guías CCN-STIC del CCN que pudieran ser de aplicación, considerando el equilibrio entre la importancia de la información que se maneja y el esfuerzo de seguridad requerido, en función de los riesgos a los que está expuesto, bajo el principio de proporcionalidad.
- Ser informado de los riesgos residuales.
- Ser consultado en relación con el impacto que puede suponer para la información y la digitalización del dato, la necesidad de paralizar un servicio en base a los riesgos detectados bajo criterios del responsable del Sistema y con la supervisión del responsable de Seguridad.
- Desplegar la operativa de la Política de Calificación de la Información, en consideración con los requisitos de la normativa implicada.
- Dictaminar respecto a los derechos de acceso a la información.
- Poner en comunicación del responsable de Seguridad cualquier variación respecto a la Información de la que es responsable, especialmente la incorporación nueva Información a su cargo.
- Considerar necesidades relacionadas con la digitalización de los datos y procesos implicados en la información de los servicios de la entidad.
- Impulsar la interoperabilidad y uso de medios electrónicos en las funciones clave de la entidad, con pleno cumplimiento de los requisitos de normativa electrónica y de seguridad.

6.2.1.3. Responsable de los Servicios

Serán funciones de este perfil:

- Determinar los requisitos del servicio prestado.
- Valorar los servicios, conforme a lo estableció en el Real Decreto 311/2022, instrucciones aplicables, así como las guías CCN-STIC del CCN que pudieran ser de aplicación, considerando el equilibrio entre la importancia de los servicios que se prestan y el esfuerzo de seguridad requerido, en función de los riesgos a los que está expuesto, bajo el principio de proporcionalidad.
- Ser informado de los riesgos residuales.
- Ser consultado en relación con la necesidad de paralizar un servicio en base a los riesgos detectados bajo criterios del responsable del Sistema y con la supervisión del responsable de Seguridad.
- Dictaminar respecto a los derechos de acceso a los servicios.
- Aceptar los riesgos residuales -que afectan a los servicios- calculados en el análisis de riesgos siempre que sus valores no sean mayores a MEDIO, y realizar su seguimiento y control.
- Poner en comunicación del responsable de Seguridad cualquier variación respecto a los Servicios de los que es responsable, especialmente la incorporación de nuevos Servicios a su cargo.

6.2.2. Estructura de supervisión

La estructura de supervisión de la seguridad se encarga de verificar la correcta implantación y operación de los requisitos de seguridad que se hayan establecido, de cara a mantener la alineación con los objetivos y de cumplir con las normas y legislación aplicable.

Forman parte de esta estructura:

- Gerencia, en calidad de representante y/o interlocutor de la alta dirección de la entidad y responsable de interlocución con esta.
- Responsable de Seguridad de la Información.

Las funciones y responsabilidades de cada una de las figuras se describen en los siguientes apartados.

6.2.2.1. Presidencia

Es la representación del compromiso formal de la Alta Dirección de la fundación con la seguridad, participando de la gobernanza y promoviendo el apoyo a los planes de seguridad que se deriven de la aplicación de esta Política.

Serán funciones clave de la Presidencia del CSI:

- Participar activamente en Comité de Seguridad, ostentando a la presidencia de este y asumiendo las responsabilidades derivadas.
- Promover la interlocución directa con los órganos de gobierno de la entidad, derivando las necesidades de seguridad y proponiendo el impulso necesario a la seguridad.
- Promover el dialogo entre los diferentes roles y responsabilidades a las personas asociadas a los planes de seguridad.
- Apoyar la formación implicados en los planes de seguridad para que adquieran el nivel de concienciación y las competencias necesarias.
- Velar por el cumplimiento con el Esquema Nacional de Seguridad.
- Facilitar las comunicaciones con otras organizaciones en materia de Seguridad de la Información.
- Promover la mejora continua en el ámbito de Seguridad de la Información.

6.2.2.2. Responsable de Seguridad de la Información

Es responsable de la definición, coordinación, difusión y verificación de los requisitos de Seguridad de la información en la Organización.

Este responsable forma parte del Comité de Seguridad, asumiendo la secretaría del Comité. Sus responsabilidades incluyen:

- Determinar las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisar la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones.
- Asesorar en materia de seguridad a los integrantes de la FECYT que así lo

requieran.

- Coordinar la interacción con otros organismos especializados.
- Tomar conocimiento y supervisar la investigación y monitorización de los incidentes de seguridad.
- Determinar las decisiones a adoptar para satisfacer las medidas de seguridad, conforme a las necesidades establecidas por los responsables de los Servicios y de la Información, del análisis y gestión de riesgos, de la información fruto del análisis de los indicadores implementados, y de las pautas del Anexo II del Esquema Nacional de Seguridad.
- Asesorar, en colaboración con el responsable del Sistema, los responsables de la Información y de los Servicios en la realización de los análisis y gestión de riesgos, elevando el informe resultado al Comité de Seguridad.
- Planificar y coordinar las auditorías internas y externas necesarias para la certificación en el ENS, así como supervisar la implantación de las correcciones que se deriven de las mismas.
- Impulsar el desarrollo del Plan Anual de Formación en Ciberseguridad, en colaboración con el Departamento de Recursos Humanos, y siguiendo las directrices del Comité de Seguridad.
- Aprobar los procedimientos de seguridad que forman parte del Mapa Normativo (y no son competencia del Comité) y poner en conocimiento del Comité de las modificaciones que se hayan realizado a lo largo del periodo en curso.
- Participar cuando sea requerido en otros órganos o grupos creados al amparo del presente.
- Apoyar la creación de la documentación de tercer nivel (Procedimientos Técnicos de Seguridad) de obligado cumplimiento.
- Mantener la documentación organizada y actualizada, gestionando los mecanismos de acceso a la misma.
- Asumir la función de secretaría del comité de seguridad y por ello, convocar, de acuerdo con la presidencia, las reuniones del Comité de Seguridad, de las que levantará acta.
- Garantizar la seguridad de los datos, implantando y haciendo cumplir las medidas, procedimientos, instrucciones y normativas establecidas en el Manual jurídico definido en la FECYT, así como sus anexos.
- Promover el mantenimiento de un listado actualizado de las personas autorizadas a acceder a los sistemas de información.
- Instar la realización de los controles periódicos establecidos para verificar el cumplimiento de la seguridad.
- Analizar los informes de auditoría, y elevar al comité y a la Alta Dirección las conclusiones y los pertinentes planes de acción.
- Promover las revisiones externas e internas de la seguridad, así como los procesos de conformidad con el Esquema Nacional de Seguridad.

6.2.3. Estructura de operación

La estructura de operación de la seguridad debe asumir la administración operativa de la seguridad de los sistemas de información, implantando en dichos sistemas las medidas

necesarias para satisfacer los requisitos de seguridad establecidos por la estructura de especificación.

Forman parte de esta estructura:

- Responsable(s) del Sistema.
- Responsable(s) de Infraestructura IT.
- Responsable(s) la Seguridad física.
- Las personas usuarias de los sistemas.

Se describen a continuación las funciones y responsabilidades de las figuras asociadas a la estructura de operación.

6.2.3.1. Responsable del Sistema

Se designará este rol en persona(s) con conocimientos de tecnología, y capacidad de operar directamente sobre el sistema, coordinar unidades de IT, servicios de ciberseguridad y entidades prestadoras de servicios digitales.

Sus funciones y responsabilidades son:

- Desarrollar, operar y mantener el sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Proporcionar asesoramiento para la determinación de la categoría del sistema, en colaboración con el responsable de Seguridad y el Comité de Seguridad.
- Garantizar que las medidas de seguridad se integren adecuadamente dentro del marco general de Seguridad de la Información.
- Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema.
- Elaborar procedimientos técnicos de seguridad de los sistemas de información.
- Participar en los órganos de gobierno que sean considerados y aprobados conforme esta política.
- Elaborar planes de continuidad de los sistemas de información.
- Adoptar las medidas correctoras derivadas de las auditorías de seguridad.
- Acordar la suspensión del manejo de determinada información o la prestación de un cierto servicio junto con el responsable de Seguridad, si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión deberá ser consultada con responsables de la Información afectada y responsables del Servicio antes de ser ejecutada.
- Participar con los restantes responsables y órganos de gobernanza en la implantación y mejora de la seguridad y asesorará cuando sea necesario, en la operatividad del sistema.

6.2.3.2. Responsable de Infraestructura IT

Se designará este rol en persona(s) con conocimientos de infraestructura y arquitectura tecnológica.

Sus funciones y responsabilidades son:

- Gestión de la infraestructura informática y de telecomunicaciones.
- Soporte a personas usuarias (microinformática y aplicaciones internas).
- Monitorización y seguridad de los sistemas.
- Colaboración en la formalización de Contrataciones (Pliegos de desarrollo software de la FECYT, Ofertas de colaboración, estimación económica…).
- Apoyo en la implantación y seguimiento de las medidas necesarias para el cumplimiento de la RGPD desde el punto de vista de la infraestructura tecnológica de la FECYT.
- Planificación y seguimiento de los proyectos.
- Análisis de requisitos y gestión de la documentación técnica.
- Coordinación de los trabajos solicitados a las empresas proveedoras.
- Coordinación de la implantación de las entregas.
- 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 los responsables de la Información afectada, los responsables del Servicio y el responsable de Seguridad antes de ser ejecutada.

6.2.3.3. Responsable de la Seguridad Física

Se designará este rol en persona(s) con conocimientos de seguridad física y de medidas de protección perimetral, riesgos a las instalaciones y a las personas. Dispondrá de conocimientos suficientes y cuando sea necesario, titulación o formación adecuada, para realizar las funciones de dirección de Seguridad, habilitaciones de seguridad, y enlace en otras normativas que impliquen medidas de seguridad.

Sus funciones y responsabilidades son:

- Coordinación de las tareas de mantenimiento y servicios generales del edificio, sus instalaciones y equipamiento.
- Seguimiento y gestión de los suministros, servicios de mantenimiento de edificios e instalaciones y gestión de residuos, subcontratados por la Fundación.
- Elaboración y gestión del presupuesto de mantenimiento y en la realización y supervisión de los planes de mantenimiento a corto, medio y largo plazo.
- Elaboración y actualización de la documentación correspondiente a las instalaciones.
- Supervisión del cumplimiento de la normativa de prevención de riesgos laborales en la ejecución de los trabajos en las instalaciones, realizando en su caso la correspondiente Coordinación de Actividades Empresariales de todos los servicios y obras contratados por la FECYT.
- Ejercicio de las funciones de organización, dirección e inspección del personal y servicios de seguridad privada contratados por la Fundación.
- Seguimiento de la implantación de los sistemas de seguridad que resulten pertinentes, así como la supervisión de su utilización, funcionamiento y conservación.
- Colaboración de los servicios de seguridad con los de las correspondientes dependencias de las Fuerzas y Cuerpos de Seguridad.

- Coordinación del trabajo de otros técnicos implicados en el mantenimiento y seguridad del edificio.
- 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 los responsables de la Información afectada, los responsables del Servicio y el responsable de Seguridad antes de ser ejecutada.

6.2.3.4. Personas usuarias de los sistemas

Toda la plantilla de la FECYT, como personas usuarias de los sistemas de información, debe conocer y cumplir esta Política de Seguridad de la Información conforme se detalla en el apartado 6.

6.2.4. Otros roles

6.2.4.1. Administradores de seguridad

Atendiendo a la estructura organizativa de la entidad, la FECYT podrá contar con un Administrador que, según las funciones que realice, puede depender del responsable del Sistema o del responsable de la Seguridad.

6.2.4.2. Persona delegada de Protección de Datos (DPD)

Serán funciones de este perfil:

- Informa y asesora al responsable del tratamiento, a la Dirección y a los empleados sobre las obligaciones derivadas del RGPD y normativa aplicable, siendo consultado de forma previa y oportuna en todas las decisiones que afecten a la protección de datos personales conforme al artículo 38.1 del RGPD.
- Supervisar el cumplimiento de la normativa de protección de datos y de las políticas internas de la Fundación en materia de protección de datos, asesorando sobre tratamientos de alto riesgo, incluyendo aquellos que impliquen colectivos vulnerables (menores, datos de salud), nuevas tecnologías (inteligencia artificial, big data, biometría), tratamientos a gran escala, videovigilancia, control laboral, transferencias internacionales, decisiones automatizadas y perfilado, promoviendo y supervisando la realización de auditorías periódicas de cumplimiento en las áreas y tratamientos que lo requieran.
- Actuar como interlocución ante la Agencia Española de Protección de Datos (AEPD) en inspecciones, requerimientos, consultas formales y procedimientos sancionadores, cooperando activamente en todo momento. Asimismo, ejercer como punto de contacto principal para cuestiones relacionadas con el tratamiento de datos personales, incluida la consulta previa prevista en el artículo 36 del RGPD cuando el tratamiento pueda implicar un alto riesgo residual tras la EIPD.
- Asesorar sobre la metodología y necesidad de las Evaluaciones de Impacto en la Protección de Datos (EIPD) cuando los tratamientos puedan entrañar un alto riesgo para los derechos y libertades de las personas conforme al artículo 35 del RGPD, supervisando su aplicación y la implementación de las medidas de mitigación

resultantes.

- Asesorar sobre la gestión de violaciones de seguridad de datos personales conforme a los artículos 33 y 34 del RGPD. Ser informado inmediatamente de cualquier brecha para evaluar el riesgo para los derechos y libertades de los interesados y asesorar sobre las obligaciones de notificación a la autoridad de control (plazo de 72 horas desde el conocimiento) y comunicación a los interesados (cuando entrañe alto riesgo). Supervisar el mantenimiento del registro de violaciones de seguridad conforme al artículo 33.5 del RGPD
- Asistir y supervisar el mantenimiento del Registro de Actividades de Tratamiento (RAT) conforme al artículo 30 del RGPD y su publicación según lo dispuesto en el artículo 31.2 de la LOPDGDD, verificando su actualización periódica y su adecuación a la realidad de los tratamientos efectuados por la Fundación.
- Asesorar y supervisar el procedimiento de atención al ejercicio de los derechos de las personas interesadas (acceso, rectificación, supresión, limitación, portabilidad, oposición y a no ser objeto de decisiones automatizadas) conforme a los artículos 15 a 22 del RGPD, garantizando el cumplimiento de los plazos legales (un mes ampliable dos meses adicionales) y la adecuación de las respuestas.
- Promover la concienciación y formación del personal en materia de protección de datos, colaborando en el diseño e impartición de programas formativos adaptados a las distintas áreas y niveles de la organización, fomentando una cultura de privacidad desde el diseño y responsabilidad proactiva.
- Emitir dictámenes especializados en régimen de consulta preceptiva sobre servicios, proyectos, tratamientos de alto riesgo, contratos con encargados del tratamiento, acuerdos de corresponsabilidad, transferencias internacionales de datos, uso de tecnologías emergentes y cualquier decisión estratégica que implique tratamiento de datos personales. El responsable del tratamiento garantizará la consulta previa y oportuna al DPD conforme al artículo 38.1 del RGPD, debiendo tener debidamente en cuenta su criterio especializado. La Fundación, como norma de buena gobernanza, tendrá documentadas las razones cuando se adopten decisiones que se aparten del dictamen del DPD. Cuando el DPD aprecie la existencia de una vulneración relevante en materia de protección de datos, debe documentarlo y comunicarlo inmediatamente a la Dirección de la Fundación.

6.2.5. Servicios de Soporte

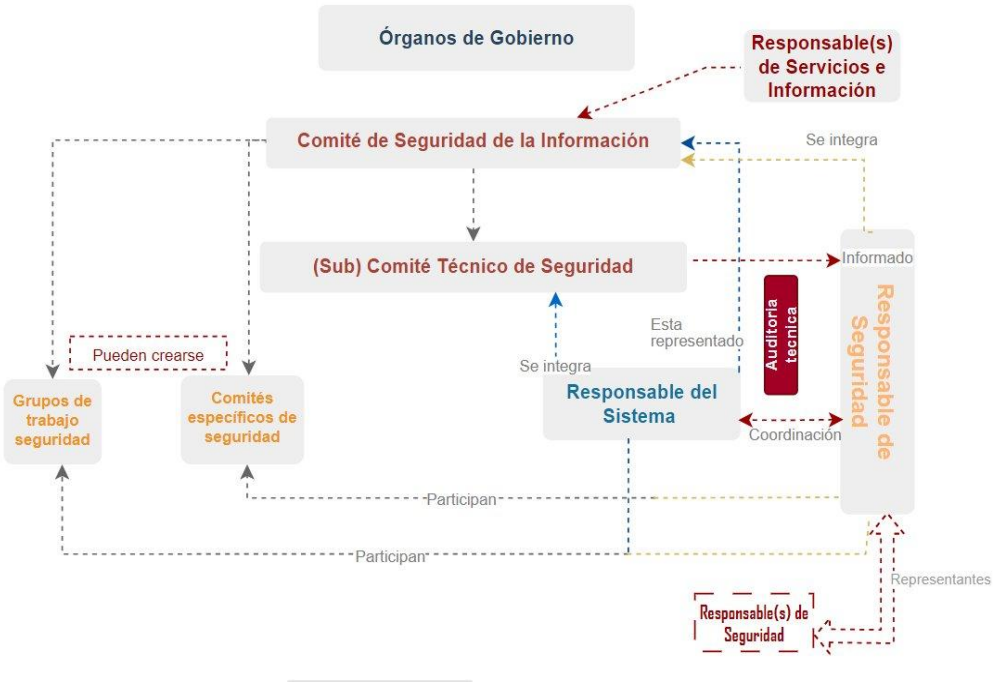
La FECYT dispone de un Equipo de Medidas Técnicas, responsable de la implantación y mantenimiento de las medidas de seguridad aprobadas. Este equipo asume la ejecución de las actuaciones técnicas necesarias para garantizar la protección de los sistemas de información y asegurar la correcta aplicación de los controles establecidos.

Asimismo, la FECYT cuenta con un Equipo Técnico de Ciberseguridad, encargado de la supervisión continua del estado de ciberseguridad, la revisión de los registros y la atención de las alertas e incidentes comunicados a través de los canales habilitados. Este equipo mantiene una coordinación permanente con el Centro de Operaciones de Seguridad (SOC), servicio especializado que proporciona monitorización, detección y respuesta ante amenazas en tiempo real y que constituye un elemento esencial en la defensa de los activos digitales de la organización.

6.3. Reportes entre los diferentes roles y responsables

Todos los órganos y roles descritos anteriormente, y aquellos que se pudieran constituir al amparo de las facultades otorgadas por esta Política, deben interactuar en la gobernanza con fidelidad y diligencia.

En este sentido se define un modelo de sincronización y comunicación entre los distintos participantes que se resume en la siguiente figura:



7. FUNCIONES Y OBLIGACIONES

Al margen de las funciones y atribuciones que atañen a las personas que integra el esquema organizativo responsable de la seguridad, se establecen a continuación las obligaciones de la plantilla de la FECYT, así como de aquellos terceros que tengan acceso a sus sistemas de información.

7.1. Funciones y obligaciones de terceras partes

Las terceras partes que estén relacionadas con la gestión, mantenimiento o explotación de los servicios prestados por la FECYT serán hechos partícipes de esta Política de Seguridad de la Información. Las terceras partes quedarán obligadas al cumplimiento de esta Política y a las normativas que se puedan derivar de ella.

Las terceras partes podrán desarrollar sus propios procedimientos operativos para satisfacer la Política.

Se deberán establecer procedimientos específicos de comunicación y resolución de incidencias.

Las personas de terceras partes deberán recibir sesiones de concienciación, al igual que las propias de la organización.

Cuando algún aspecto de esta Política no pueda ser satisfecho por una tercera parte, el responsable de Seguridad deberá realizar un informe del riesgo en que se incurre. Ese informe deberá ser aprobado por el Comité de Seguridad con carácter previo a la adopción de medidas al respecto.

7.2. Resolución de conflictos

En caso de conflicto entre los diferentes responsables de información o de servicio que componen la estructura organizativa de la Política de Seguridad de la Información, o responsable de Seguridad y responsable del Sistema, serán resueltos por el Comité de Seguridad de la Información.

En la resolución de estas controversias se tendrán siempre en cuenta las exigencias derivadas de la protección de datos de carácter personal.

8. FORMACIÓN Y CONCIENCIACIÓN

Con carácter anual se realizará, al menos, una acción de formación y concienciación en materia de seguridad.

El objetivo de la acción formativa y de concienciación es doble:

- Mantener informadas a las personas directamente involucradas en la gestión de la información y los sistemas asociados sobre los procedimientos de seguridad existentes, riesgos identificados, medidas de protección implementadas y planes de contingencia establecidos, entre otros aspectos relevantes.
- Concienciar a la plantilla, en general, de la importancia de la seguridad y de los procedimientos básicos de manejo e intercambio de información.

El primer objetivo se asocia a Formación y el segundo a Concienciación.

Las áreas responsables determinarán el formato de la acción de Formación y Concienciación, así como sus contenidos.

9. GESTIÓN DE RIESGOS

Los servicios e infraestructuras bajo el alcance de la presente Política deberán estar sometidos a un análisis de riesgos para orientar las medidas de protección a minimizar los mismos.

Como metodología base para la realización de los análisis de riesgos se utilizará Magerit, siendo esta metodología la más recomendable para el sector público estatal.

Se utilizarán, como punto de partida, el catálogo de amenazas de seguridad previsto en la metodología. El análisis se realizará:

- Regularmente, una vez al año.
- Cuando haya cambios significativos en la información manejada.
- 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.

De acuerdo con la escala de riesgos de la metodología Magerit, el nivel de riesgo deberá situarse por debajo de nivel ALTO para considerarse de forma automática como aceptable (el riesgo residual máximo debe ser MEDIO). Los valores de riesgo residual mayores a MEDIO deberán ser aceptados explícitamente por el Comité de Seguridad, previa justificación de la conveniencia de su aceptación.

Para los valores de riesgo residual que no sean aceptables se deberá elaborar el correspondiente Plan de Tratamiento que permita llevar los valores de riesgo a valores aceptables.

10. DATOS DE CARÁCTER PERSONAL

La FECYT en su política de protección de datos, mantiene un compromiso de cumplimiento de la legislación vigente en materia de tratamiento de datos personales con el objeto de garantizar que el tratamiento de los datos de carácter personal se realiza conforme al Reglamento (UE) 2016/679 General de Protección de Datos (RGPD), Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD), así como de la jurisprudencia existente en materia de protección de datos de carácter personal, y de los informes y resoluciones de la Agencia Española de Protección de Datos (AEPD).

La FECYT aplicará los principios incluidos en el RGPD cuando realice tratamientos datos de carácter personal:

- Principio de “licitud, transparencia y lealtad”: los datos deberán ser tratados de manera lícita, leal y transparente para el interesado.
- Principio de “limitación de la finalidad”: implica, por una parte, la obligación de que los datos sean tratados con una o varias finalidades determinadas, explícitas y legítimas y, por otra, que se prohíbe que los datos recogidos con unos fines determinados, explícitos y legítimos sean tratados posteriormente de una manera incompatible con esos fines.
- Principio de “minimización de datos”: la FECYT solo recogerá datos de carácter personal cuando sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.
- Principio de “exactitud”: los datos deben ser exactos y, si fuera preciso, actualizados, debiendo adoptarse por parte de la FECYT todas las medidas

razonables para que se rectifiquen o supriman los datos inexactos en relación con los fines que se persiguen.

- Principio de "limitación del plazo de conservación": solo pueden tratarse los datos adecuados, pertinentes y necesarios para una finalidad, la conservación de esos datos debe limitarse en el tiempo al logro de los fines que el tratamiento persigue. Una vez que esas finalidades se han alcanzado, los datos deben ser borrados o, al menos, desprovistos de todo elemento que permita identificar a las personas interesadas.
- Principio de "integridad y confidencialidad": obligación de actuar proactivamente con el objetivo
de proteger los datos que manejan frente a cualquier riesgo que amenace su seguridad.
- Principio de "responsabilidad proactiva": implica aplicar por parte de la FECYT las medidas técnicas y organizativas apropiadas para garantizar y estar en condiciones de demostrar que el tratamiento de datos personales se lleva a cabo de conformidad con el RGPD.

La FECYT aplicará medidas de seguridad para garantizar el derecho fundamental a la protección de datos garantizando la confidencialidad, la integridad y la disponibilidad de los datos personales. Para garantizar estos tres factores de la seguridad la FECYT aplicará las medidas de seguridad necesarias adecuadas al nivel de los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas conforme al artículo 32 del RGPD.

En relación con las medidas de seguridad en el ámbito del sector público, la FECYT cumplirá con la disposición adicional primera de la LOPDGDD, que señala que los responsables enumerados en el artículo 77.1 de la citada ley orgánica, entre los que se encuentran las fundaciones del sector público como la FECYT , deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado.

La FECYT dispondrá de un Registro de Actividades del Tratamiento de datos de carácter personal que incluirá los contenidos regulados en el artículo 30 del RGPD y lo hará público en su portal de transparencia en aplicación del artículo 31.2 de la LOPDGDD.

11. GESTIÓN DE INCIDENTES DE SEGURIDAD

La FECYT dispondrá de un procedimiento para la gestión ágil de los eventos e incidentes de seguridad que supongan una amenaza para la información y los servicios.

Este procedimiento se integrará con otros relacionados con los incidentes de seguridad de otras normas sectoriales como la de protección de datos personales u otra que afecte al organismo para coordinar la respuesta desde los diferentes enfoques y comunicar a los diferentes organismos de control sin dilaciones indebidas y, cuando sea preciso, a las Fuerzas y Cuerpos de Seguridad el Estado o los juzgados.

12. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política de Seguridad de la Información se desarrollará mediante la elaboración de otras políticas o normativas de seguridad que aborden aspectos específicos. A raíz de dichas políticas y normativas se podrán desarrollar procedimientos que describan la forma de llevarlas a cabo.

La documentación de políticas y normativas de seguridad, así como esta Política de Seguridad de la Información, se encontrará a disposición de todo el personal de la Fundación que necesite conocerla y, en particular, del personal que utilice, opere o administre los sistemas de información y comunicaciones, o la información misma albergada en dichos sistemas, o los servicios prestados por la FECYT.

12.1. Estructura normativa

La Política de Seguridad de la Información es de obligado cumplimiento y se estructura en los siguientes niveles relacionados jerárquicamente:

1. Primer nivel: Política de Seguridad de la Información.
2. Segundo nivel: Normativas de Seguridad de la Información.
3. Tercer nivel: Procedimientos e Instrucciones Técnicas de Seguridad de la Información.
4. Cuarto nivel: Informes, registros y evidencias electrónicas.

La estructura jerárquica permite adaptar con eficiencia los niveles inferiores a los cambios en los entornos operativos de la FECYT, sin necesidad de revisar su estrategia de seguridad.

El personal de la FECYT tendrá la obligación de conocer y cumplir, además de la Política de Seguridad de la Información, todas las Normativas, los Procedimientos e Instrucciones Técnicas de Seguridad de la Información que puedan afectar a sus funciones.

La Política, las Normativas, los Procedimientos e Instrucciones Técnicas de Seguridad de la Información estarán disponibles para todo el personal en la Intranet de la FECYT según vayan siendo aprobadas.

1. Primer nivel: Política de Seguridad de la Información
   Este documento es de obligado cumplimiento por todo el personal, interno y externo, de la FECYT, recogido en el presente documento y aprobado por el Comité de Seguridad de la Información. Se elevará para su información al Comité de Dirección.

2. Segundo nivel: Normativas de Seguridad de la Información
   a. De obligado cumplimiento de acuerdo con el ámbito organizativo, técnico o legal correspondiente.
   b. La responsabilidad de aprobación de los documentos redactados en este nivel será competencia del responsable de Seguridad bajo la supervisión

del Comité de Seguridad.

3. Tercer nivel: Procedimientos e Instrucciones Técnicas de Seguridad de la Información
   a. 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.
   b. La responsabilidad de aprobación de estos procedimientos técnicos es del responsable del Sistema de Información, bajo la supervisión y asesoramiento del responsable de Seguridad.
   c. En caso de que los procedimientos afectaran a varios sistemas de información será responsabilidad del responsable de Seguridad el aprobarlos.

4. Cuarto Nivel: Informes, registros y evidencias electrónicas
   a. El cuarto nivel está constituido por 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.
   b. La responsabilidad de que existan este tipo de documentos es de cada uno de los responsables de los Servicios de Información en su ámbito.

5. Otra documentación
   a. Para el mejor cumplimiento de lo establecido en el ENS, se seguirán las correspondientes guías de seguridad de las tecnologías de la información y la comunicación (guías CCN-STIC), que se incorporarán al conjunto documental.
   b. Los reglamentos, órdenes, decretos y resto de legislación relativa a la protección de datos personales tanto procedentes de la Unión Europea como del Estado Español.

13. INCUMPLIMIENTO

El incumplimiento de la presente Política y de los deberes y responsabilidades en materia de seguridad derivados, podrá acarrear el inicio de las medidas disciplinarias que procedan, sin perjuicio de las responsabilidades legales correspondientes.

14. REVISIÓN Y APROBACIÓN

De conformidad con el artículo 31 del ENS, así como su Anexo III y las guías de aplicación del CCN-STIC, y bajo un ciclo de mejora continua, se hace necesario someterse a un proceso de conformidad con la citada norma, que requerirá una auditoría externa acreditada. El proceso de certificación deberá realizarse cada 2 años, o antes de este periodo, si existieran cambios sustanciales en el sistema.

Las presente Política, puede requerir modificaciones y en su caso, cambios o adaptaciones siendo en todo caso necesario ser elevada para su aprobación al Comité de Seguridad de la Información. El responsable de Seguridad será el encargado de velar por las revisiones de la Política, al menos, una vez al año.

Esta Política tiene vigencia desde el día de su aprobación por el órgano competente que se defina en esta Política y hasta que sea modificada o sustituida por otra norma de igual rango.

La presente Política de Seguridad de la Información ha sido aprobada por el Comité de Seguridad como órgano competente, siendo elevada para su información por el Comité de Dirección y en su caso, Patronato.

ANEXO I. MARCO NORMATIVO

Esta política se enmarca en el siguiente contexto normativo:

1. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
2. Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
3. 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).
4. Reglamento Europeo de Firma Electrónica (eIDAS 2). Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024.
5. Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
6. Ley 11/2022, de 28 de junio, General de Telecomunicaciones.
7. Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
8. Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
9. Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público.
10. Ley 38/2003, de 17 de noviembre, General de Subvenciones.
11. Ley 4/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación.
12. Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
13. Ley 2/2011, de 4 de marzo, de Economía Sostenible.
14. Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
15. Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.
16. Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.
17. Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.
18. 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.
19. 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.
20. Real Decreto-ley 14/2022, de 1 de agosto, de medidas de sostenibilidad económica en el ámbito del transporte, en materia de becas y ayudas al estudio, así como de medidas de ahorro, eficiencia energética y de reducción de la dependencia energética del gas natural.
21. Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.
22. 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.

23. Ley 18/2014, de 15 de octubre, de aprobación de medidas urgentes para el crecimiento, la competitividad y la eficiencia.
24. Orden HAP/2425/2013, de 23 de diciembre, por la que se publican los límites de los distintos tipos de contratos a efectos de la contratación del sector público a partir de 1 de enero de 2014.
25. Orden PCM/466/2022, de 25 de mayo, por la que se publica el Acuerdo del Consejo de Ministros de 24 de mayo, por el que se aprueba el plan de medidas de ahorro y eficiencia energética de la Administración General del Estado y las entidades del sector público institucional estatal.
26. Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.
27. Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.
28. Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.
29. Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.
30. Jurisprudencia existente en materia de protección de datos de carácter personal.

Guias de referencia

1. CCN-STIC-402: Organización y Gestión para la Seguridad de los Sistemas TIC. 2006.
2. CCN-STIC-801: ENS - Responsabilidades y funciones. 2019.
3. CCN-STIC-805: ENS - Política de Seguridad de la Información. 2011
4. CCN-STIC-830: ENS - Ámbito de aplicación del Esquema Nacional de Seguridad. 2016
5. Informes y resoluciones de la Agencia Española de Protección de Datos (AEPD)

ANEXO II. GLOSARIO

CCN-CERT

El CCN-CERT es la Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN.

Guías CCN-STIC

Las Series CCN-STIC son normas, instrucciones, guías y recomendaciones desarrolladas por el Centro Criptológico Nacional con el fin de mejorar el grado de ciberseguridad de las organizaciones. Periódicamente son actualizadas y completadas con otras nuevas, en función de las amenazas y vulnerabilidades detectadas por el CCN-CERT.