Política de Seguridad de la Información

Edición Nº	Fecha de emisión
v1.3	**Enero 2022**

C/ PINTOR MURILLO 15
ALCOBENDAS - 28100 MADRID

TEL.: 91-425-09-09
FAX: 91-571-21-72

Preparado por:	Revisado por:
Ingenia	**Responsable de Seguridad de FECYT**

Edición Nº	Fecha de emisión
v1.3	**Enero 2022**

CONTROL DE VERSIONES

Versión	Fecha	Editor	Descripción del cambio
1.0	01/08/2018	Ingenia	Redacción inicial (primera edición)
1.1	15/10/2019	Julián Oliveros Juan José Pérez Javier Domingo	Primera revisión de la política y aprobación de su versión final
1.2	24/01/2020	Juan José Pérez Florencio Núñez	Listado de proyectos vinculados al inventario de activos Eliminación de normativa derogada
1.3	Dic 2021	Antonio Jesús Sánchez Padial	Ajustes en la definición de FECYT Actualización de normativa Simplificación de la Organización de la Seguridad Reduccción de miembros en el Comité de Seguridad Inclusión de la Dirección General en la Estructura de Supervisión Eliminación de alusiones a las normas UNE/ISO 27001 y 27002 Eliminación de alusiones al Sistema de Gestión de la Seguridad de la Información Modificación de cabecera y pie de página
1.4	Enero 2022	Antonio Jesús Sánchez Padial	Incorporación del Director de Proyectos Estratégicos al Comité de Seguridad.

Contenido

0 Introducción

Este documento constituye la Política de Seguridad de la Información de la **Fundación Española para la Ciencia y la Tecnología, FSP (FECYT)**, en cumplimiento del artículo 11 del Real Decreto 3/2010 de 8 de enero, por el que se regula los requisitos mínimos de Seguridad en el ámbito de la Administración Electrónica, y de la medida de seguridad org.1 contemplada en el Anexo II de dicho Real Decreto.

En este sentido, el mencionado artículo 11 establece que "*Todos los órganos superiores de las Administraciones públicas deberán disponer formalmente de su política de seguridad, que será aprobada por el titular del órgano superior correspondiente.*"

La estructura de este documento sigue las pautas establecidas por la guía CCN-STIC-805 para la redacción de la Política de Seguridad de la Información en el ámbito del Esquema Nacional de Seguridad.

La Política de Seguridad de la Información recoge la postura de FECYT en cuanto a la seguridad de la información y establece los criterios generales que deben regir la actividad del organismo en cuanto a la seguridad.

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

Los sistemas 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. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios.

1 La Fundación Española para la Ciencia y la Tecnología (FECYT)

La Fundación Española para la Ciencia y la Tecnología (en adelante FECYT) es una fundación del sector público (FSP) dependiente del Ministerio de Ciencia e Innovación.

Su fin fundacional es fomentar la investigación científica de excelencia así como el desarrollo y la innovación tecnológica necesarios para incrementar la competitividad de la industria española y la mejora de la calidad de vida de la ciudadanía, propiciando para ello la colaboración entre los agentes implicados en actividades de I+D+I y la difusión y comunicación de los resultados y actuaciones realizadas en investigación e innovación.

La Fundación 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 2013-2016 y la Ley 14/2011 de 1 de junio de la Ciencia, la Tecnología y la Innovación. La ajustada situación de recursos humanos disponibles exige el establecimiento claro de prioridades en una programación ajustada y eficaz.

La actividad principal de 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 las necesidades de los agentes del Sistema Español de Ciencia, Tecnología e Innovación.

2 Marco normativo

Esta política se enmarca en el siguiente marco normativo:

1. Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. BOE de 29 de enero de 2010.
2. Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas.
3. Ley 40/2015, de 1 de octubre de Régimen Jurídico del Sector Público.
4. Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos .
5. Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común[1].
6. 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 - RGPD).
7. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).
8. Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el texto refundido de la Ley de Contratos del Sector Público[1].
9. 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.
10. Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
11. Ley 23/2006, de 7 de julio, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril.
12. Ley 2/2011, de 4 de marzo, de Economía Sostenible.
13. Ley 59/2003, de 19 de diciembre, de firma electrónica.
14. Ley 33/2003, de 3 de noviembre, del Patrimonio de las Administraciones Públicas.
15. Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
16. 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 del 1 de enero de 2014.
17. Real Decreto-ley 8/2014, de 4 de julio, de aprobación de medidas urgentes para el crecimiento, la competitividad y la eficiencia.
18. Ley 18/2014, de 15 de octubre, de aprobación de medidas urgentes para el crecimiento, la competitividad y la eficiencia.
19. Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción de Seguridad de conformidad con el Esquema Nacional de Seguridad.
20. 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.
21. 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.
22. 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. 2016Informes y resoluciones de la Agencia Española de Protección de Datos (AEPD)

3 Política General de Seguridad

El objeto de la presente Política es establecer la postura de FECYT respecto a la Seguridad que afecta a los procesos relacionados con el desempeño de sus funciones y, muy particularmente, con los relacionados con la administración electrónica, tanto desde el punto de vista de los usuarios de los servicios, como desde el punto de vista interno, para la gestión de la propia Entidad.

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.

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).

La política de FECYT es la de contrarrestar las amenazas mencionadas anteriormente con los medios suficientes, dentro de las posibilidades presupuestarias. 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 los mismos, 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 Esquema Nacional de Seguridad 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 los usuarios, 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, 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 los usuarios, 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

Esta Política de Seguridad de la Información es de aplicación a todos los servicios prestados por FECYT que se apoyen en las Tecnologías de la Información y las Comunicaciones, así como a todo el personal, sin excepciones.

5 Organización de la seguridad

La organización de la seguridad está basada en la Guía CCN-STIC-402: Organización y Gestión para la Seguridad de los Sistemas TIC del Centro Criptológico Nacional.

Se establecerán las siguientes estructuras:

- 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.

5.1 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:

- La Dirección General
- El/La Responsable de Seguridad de la Información.
- El Comité de Seguridad de la Información.
- Los y las Responsables de la Información y del Servicio.

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

5.1.1 Dirección General

La Dirección General de FECYT manifiesta su compromiso formal con el apoyo a los planes de seguridad que se deriven de la aplicación de esta Política. Dicho apoyo se concretará en:

- proporcionar los recursos humanos y económicos necesarios, dentro de las posibilidades presupuestarias;
- asignar roles y responsabilidades a las personas asociadas a los planes de seguridad;
- apoyar la formación de los recursos humanos 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.

El compromiso con el apoyo a los planes se manifiesta con la aprobación del presente documento.

5.1.2 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, tomando el papel de Secretario del Comité y, por tanto, es el encargado de elevar a dicho Comité los asuntos de interés relacionados con la seguridad de la información.

Sus responsabilidades incluyen:

- Convocar y coordinar las reuniones del Comité de Seguridad, en el que participará como Secretario.
- Establecer 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.
- Supervisar el cumplimiento de la Política de Seguridad de la información de la FECYT, así como de sus normas y procedimientos derivados.
- Planificación de los objetivos estratégicos de FECYT en materia de ciberseguridad en el Plan Estratégico, y de la actividad anual en los Planes de Actuación. Propondrá a Recursos Humanos los objetivos en materia de ciberseguridad valorables para la promoción y/o retribuciones especiales del personal.
- Coordinar y controlar las medidas de Seguridad de la Información. Junto al Responsable del Sistema diseñará e implantará los indicadores necesarios para medir la eficacia y eficiencia de las medidas implantadas.

- Mantener un registro de incidentes de seguridad. Investigar y analizar los incidentes de seguridad y verificar el cumplimiento de los protocolos de seguimiento de los mismos, y de la ejecución de las actuaciones que se establezcan a raíz de estos.
- Supervisar y coordinar las crisis (situaciones excepcionales) de ciberseguridad en la FECYT.
- Promover, coordinar y dar soporte a los análisis periódicos de riesgos de seguridad de los Responsables de los Servicios y de la Información. Presentar el resultado de estos análisis al Comité de Seguridad, dentro del plan de Gestión de Riesgos de FECYT.
- Planificará y coordinará las auditorías internas y externas necesarias para la certificación en el ENS. Colaborará con las mismas, y supervisará la implantación de las correcciones que se deriven de las mismas.
- Desarrollo del Plan Anual de Formación en Ciberseguridad, en colaboración con el Departamento de Recursos Humanos, y bajo las pautas del Comité de Seguridad.
- Desarrollo y evolución de la documentación de seguridad de segundo nivel (Normativa de Seguridad), que será aprobada por el Comité de Seguridad.
- Aprobará la documentación de seguridad de tercer nivel (Procedimientos e Instrucciones Técnicas de Seguridad), que será desarrollada por el Responsable del Sistema.
- Mantendrá organizada y actualizada la documentación de seguridad, asegurando el acceso a la misma al personal de la organización.

El Responsable de Seguridad de la Información será nombrado por la Dirección General de FECYT.

5.1.3 Comité de Seguridad de la Información

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

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:

- Informar regularmente del estado de la seguridad a la Dirección General de FECYT, al menos con carácter semestral.
- Revisar regularmente la Política de Seguridad de la Información y proponer cambios, si procede.
- Aprobar las Normativas de Seguridad que se deriven de la Política de Seguridad de la Información (documentación de segundo nivel) y presentarla al Comité de Dirección.
- Elaborar y proponer los requisitos de formación para el personal clave que maneja información, sistemas e infraestructuras físicas.
- Proponer para su aprobación los planes de mejora de la seguridad que surjan a raíz de los análisis de riesgos realizados.
- Seguir el desarrollo de los planes de acción aprobados.
- 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.

- Analizar incidentes de seguridad significativos (crisis de ciberseguridad). Decidir qué hacer a raíz de ellos. Algunos pueden conllevar una actuación con gasto, en cuyo caso se propondría para su aprobación.
- Analizar información de indicadores de seguridad que pudiera haber definidos. Tomar decisiones en caso de desviación respecto a los umbrales establecidos.
- Proponer soluciones de seguridad que deban tener un presupuesto aprobado.

Serán miembros fijos del Comité de Seguridad:

- El/La Director/a Gerente de FECYT.
- El/la Director/a de Proyectos Estratégicos de FECYT.
- El/La Coordinador/a de Seguridad y Mantenimiento.
- El/La Delegado/a de Protección de Datos.
- El/La Responsable de Seguridad de la Información, que actuará como secretario/a del Comité.

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.

5.1.4 Responsables de la Información y del Servicio

La figura de los Responsables de la Información y del Servicio establecerán el nivel de seguridad que la información y los servicios prestados por FECYT requieren, en base a sus exigencias en cuanto a disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad considerando el impacto que tendría en la ciudadanía y en la propia Organización la falta de alguno de esos aspectos.

Serán Responsables de la Información y del Servicio los responsables de cada uno de los departamentos de FECYT:

- Dirección Internacional.
- Políticas Europeas.
- Cultura Científica y de la Innovación.
- Gestión del Museo Nacional de Ciencia y Tecnología.
- Gestión de la Información Científica.
- Estudios e Indicadores.
- Financiero.
- Recursos Humanos.

La Dirección General de FECYT podrá nombrar Responsables de la Información y del Servicio asociados a proyectos específicos de la organización.

Sus responsabilidades son:

- Clasificar la información conforme a los criterios y categorías establecidas en el Esquema Nacional de Seguridad.
- Determinar los niveles de seguridad de los servicios en cada dimensión de seguridad dentro del marco del Esquema Nacional de Seguridad.

- Realizar los análisis de riesgos preceptivos, y seleccionar las salvaguardas a implantar, con la participación y asesoramiento del Responsable de Seguridad de la Información y del Responsable del Sistema de Información.
- Aceptar los riesgos residuales calculados en el análisis de riesgos, y realizar su seguimiento y control.

5.2 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:

- El/la Responsable del Sistema de Información
- Los usuarios de los sistemas

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

5.2.1 Responsable del Sistema de Información

El o la Responsable del Sistema de Información será el Director/a de Tecnología y Sistemas de la FECYT.

Sus funciones y responsabilidades son:

- Definir, en coordinación con el Responsable de Seguridad de la Información, las especificaciones funcionales de seguridad de los Sistemas de Información de la Organización.
- Garantizar que en el diseño de sistemas de información y redes de comunicaciones se contemplen desde el principio los aspectos necesarios de seguridad de la información en cuanto a disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad.
- Revisar que la configuración de seguridad tras la instalación de un sistema nuevo es la adecuada.
- Revisar que la configuración de seguridad tras los cambios en un sistema sigue siendo la adecuada.
- Implantar y verificar el funcionamiento de las medidas de seguridad que resulten de los planes de tratamiento de riesgos o planes de acciones correctivas a raíz de las auditorías de seguridad de la información.
- Verificar el correcto funcionamiento de los indicadores de seguridad de la información.
- Realizar auditorías técnicas periódicas para verificar el funcionamiento de las medidas y cumplimiento de los requisitos de seguridad establecidos. Estas auditorías pueden ser llevadas a cabo por personal interno o externo a la FECYT.

5.2.2 Usuarios de los sistemas

Todo el personal de FECYT, como usuarios y usuarias de los sistemas de información Política de Seguridad de la Información conforme se detalla en el apartado 6.

6 Funciones y obligaciones

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

6.1 Funciones y obligaciones del personal

Todo el personal de FECYT que tenga algún tipo de relación con el uso, la gestión, mantenimiento y explotación de la información y de los servicios prestados sobre ella, tiene la obligación de conocer la Política de Seguridad de la Información y cumplirla. El Comité de Seguridad dispondrá los medios para que esta Política llegue a los interesados.

Todo este personal deberá asistir a sesiones de concienciación en materia de seguridad, las cuales se establecerán en el plan de formación y concienciación anual.

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

6.2 Funciones y obligaciones de terceras partes

Las terceras partes que estén relacionadas con la gestión, mantenimiento o explotación de los servicios prestados por 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 de incidencias para que los terceros afectados puedan reportarlas.

El personal de las terceras partes deberá recibir sesiones de concienciación, tal como se exige para el personal propio.

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 riesgo deberá ser aceptado por el Comité de Seguridad.

6.3 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, éste será resuelto por el superior jerárquico de los mismos con la mediación del Responsable de Seguridad de la Información, elevándose para su resolución al Comité de Seguridad de la Información en caso de no llegar a un acuerdo.

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

7 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 informado al personal más directamente relacionado con el manejo de información y los sistemas que la tratan sobre los procedimientos existentes de seguridad, riesgos, medidas de protección, planes de protección, etc.
- concienciar al personal, 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.

8 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 nacional.

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). 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.

9 Datos de carácter personal

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 a 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 los interesados.
- 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 se 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.

10 Terceras partes

Cuando FECYT utilice servicios o maneje información de terceros, les hará partícipes de esta Política de Seguridad de la Información. El Comité de Seguridad de la Información establecerá canales para reporte y coordinación de los respectivos Comités de Seguridad y establecerá procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando FECYT preste servicios a otros organismos o ceda información a terceros, les hará partícipe de esta Política de Seguridad de la Información y de las Instrucciones y Procedimientos que atañan a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se exigirá que el personal de terceros esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

11 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 organización que necesite conocerla y, en particular, el 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 FECYT.

12 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 FECYT, sin necesidad de revisar su estrategia de seguridad.

El personal de 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 todos los empleados en la Intranet de FECYT según vaya 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 FECYT, recogido en el presente documento y aprobada por la Dirección General de FECYT.

2) **Segundo nivel: Normativas de Seguridad de la Información**

   De obligado cumplimiento de acuerdo con el ámbito organizativo, técnico o legal correspondiente.

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

3) **Tercer nivel: Procedimientos e Instrucciones Técnicas de Seguridad de la Información**

   Documentos técnicos orientados a resolver las tareas, consideradas críticas por el perjuicio que causaría una actuación inadecuada, de seguridad, desarrollo, mantenimiento y explotación de los sistemas de información.

   La responsabilidad de aprobación de estos procedimientos técnicos es del Responsable del Sistema de Información correspondiente, bajo la supervisión y asesoramiento del Responsable de Seguridad.

   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**

   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.

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

5) **Otra documentación**

   Se podrá seguir en todo momento los procedimientos, normas e instrucciones técnicas STIC, así como las guías CCN-STIC de las series 400, 500, 600 y 800.

   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 Revisión y aprobación

La Política de Seguridad de la Información será revisada, al menos, cada dos años.

La presente Política de Seguridad de la Información fue aprobada por la Dirección General de FECYT.

Fdo.: Immaculada Aguilar Nàcher
Cargo: Directora General de FECYT

Fin del Documento