Elaborada por:	Aprobada por:
Responsable de Seguridad	Dirección
Aprobación y entrada en vigor	
Texto aprobado a fecha de firma por la Dirección. Esta Política de Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.	
Propietario:	
Comité de Seguridad de la Información	

1. INTRODUCCIÓN

Fundación EOI, F.S.P depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad, confidencialidad, autenticidad o trazabilidad de la información tratada o los servicios prestados.

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

En cumplimiento del artículo 12 del Real Decreto del ENS, la presente Política de Seguridad se establecerá de acuerdo con los principios básicos:

- Organización e implantación del proceso de seguridad.
- Análisis y gestión de los riesgos.
- Gestión de personal.
- Profesionalidad.
- Autorización y control de los accesos.
- Protección de las instalaciones.
- Adquisición de productos.
- Seguridad por defecto.
- Integridad y actualización del sistema.
- Protección de la información almacenada y en tránsito.
- Prevención ante otros sistemas de información interconectados.
- Registro de actividad.
- Incidentes de seguridad.
- Continuidad de la actividad.
- Mejora continua del proceso de seguridad.

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

reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

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

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

1.1 PREVENCIÓN

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

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

1.2 DETECCIÓN

Dado que los servicios se puede degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

1.3 RESPUESTA

Los departamentos deben:

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

1.4 RECUPERACIÓN

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

2. ALCANCE

Esta política se aplica a todos los sistemas de información que soportan el servicio de formación en abierto, programas en materia de formación profesional como Centro de referencia Nacional (CRN), programas formativos financiados a través de fondos públicos y programas de formación In-company, prestado por Fundación EOI, F.S.P.

3. MISIÓN

EOI es una fundación que presta servicios de formación dirigida y enfocada a las necesidades del cliente, adaptando la oferta formativa a las tendencias del entorno.
Nuestras prioridades son:

- Formar y/o asesorar a los y las profesionales, actuales y futuros, en un nuevo modelo de liderazgo colaborativo que aúne capacidad emprendedora, espíritu creativo e innovador y voluntad de cooperación.
- Identificar y generar oportunidades de colaboración entre el sector público, el tejido empresarial y la sociedad.
- Adelantarse a las necesidades formativas y habilidades del profesional del futuro en un entorno global.
- Alojar a estudiantes, preferentemente universitarios, ofreciendo un clima de convivencia, estudio y valores, promoviendo la formación cultural, científica y humanística de los y las colegiales.

4. MARCO NORMATIVO

Fundación EOI, F.S.P se encuentra sujeto a la siguiente normativa en la provisión de los servicios prestados a sus clientes:

- REGLAMENTO (UE) No 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (reglamento General de Protección de Datos), de aplicación al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.
- Prevención de Riesgos Laborales Ley 31/1995 de 8 de noviembre y Real Decreto 39/1997 de 17 de enero, por el que se aprueba el Reglamento de los Servicios de Prevención.
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI-CE).
- RD-ley 13/2012 de 30 de marzo, ley de cookies.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad
- El marco de referencia que da cobertura legal a este documento se establece en las siguientes secciones del 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 (en adelante, ENS):

- ENS. Artículo 13. Organización e implantación del proceso de seguridad
  La seguridad deberá comprometer a todos los miembros de la organización. La política de seguridad, en aplicación del principio de diferenciación de responsabilidades a que se refiere el artículo 11 y según se detalla en la sección 3.1 del anexo II, deberá ser conocida por todas las personas que formen parte de la organización e identificar de forma inequívoca a los responsables de velar por su cumplimiento.
- ENS. Anexo II
  - ✓ Medidas de Seguridad Marco organizativo [org]
  - ✓ Política de seguridad [org.1]

EOI cuenta con un procedimiento de legislación aplicable, definido en el documento FPA PS09_ Política de Cumplimiento legal, y con una base de datos que recoge la legislación actualizada.

5. ORGANIZACIÓN DE LA SEGURIDAD

5.1 COMITÉ: FUNCIONES Y RESPONSABILIDADES

El Comité de Seguridad la Información estará formado por los Responsables de la información y del servicio, el Responsable de Seguridad y el Responsable del Sistema.
El Comité tendrá las siguientes funciones:

- Coordina todas las actividades relacionadas con la seguridad de las TIC
- Es responsable de la redacción de la Política de Seguridad
- Es responsable de la creación y aprobación de las normas que enmarcan el uso de los servicios TIC
- Aprobará los procedimientos de actuación en lo relativo al uso de los servicios TIC
- Aprobará los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de las TIC.

5.2 ROLES: FUNCIONES Y RESPONSABILIDADES

Los Responsables de la Información tendrán las siguientes funciones:

- Velar por el buen uso de la información y, por tanto, de su protección
- Determinar los requisitos de Seguridad de la información tratada en la Organización.
- Valorar las consecuencias de un impacto negativo sobre la seguridad de la información.
- Proteger el del uso que se da a la información.
- Trabajo en colaboración con el Responsable de Seguridad y el del Sistema para el mantenimiento del Sistema de Información catalogado según el Anexo I del ENS.

Los Responsables de los Servicios tendrán las funciones de:

- Elaborar y gestionar los requisitos de seguridad para la prestación de los servicios.
- Trabajo en colaboración con el Responsable de Seguridad y el del Sistema para el mantenimiento del Sistema de Información catalogado según el Anexo I del ENS

El Responsable del Sistema tendrá las funciones de:

- Gestionar los requisitos técnicos de seguridad de los sistemas de información.
- Desarrollar, operar y mantener el Sistema durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Realizar el análisis y gestión de riesgos en el Sistema
- Implantar y controlar las medidas específicas de seguridad del Sistema y cerciorarse de que éstas se integran adecuadamente dentro del marco general de Seguridad.

- Determinar la categoría del sistema según el procedimiento descrito en el Anexo I del ENS y determinar las medidas de seguridad que deben aplicarse según se describe en el Anexo II del ENS.
- Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.

El Responsable de Seguridad tendrá las siguientes funciones:

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas TIC en su ámbito de responsabilidad.
- Verificar que las medidas de seguridad establecidas son adecuadas para la protección de la información manejada y los servicios prestados.
- Elaborar y analizar la documentación relacionada con la seguridad del sistema.
- Monitorizar el estado de seguridad del Sistema.

El Administrador de la Seguridad del Sistema tendrá por funciones las siguientes:

- La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema de Información.
- La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.
- Informar a los Responsables de la Seguridad y/o del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

Todo el personal de Fundación EOI, F.S.P será responsable de cumplir con la presente Política de Seguridad de la Información dentro de su área de trabajo, así como de aplicar toda la información documentada de los controles y medidas de seguridad del ENS en sus actividades laborales que afecten a su desempeño en seguridad de la información.

5.3 PROCEDIMIENTOS DE DESIGNACIÓN

El Responsable de Seguridad, el Responsable del Sistema y los Responsable de la Información y de los Servicios serán nombrados por la Dirección a propuesta del Comité de Gestión de la Seguridad de la Información. Los nombramientos se revisarán cada 2 años o cuando el puesto quede vacante.

5.4 PROCEDIMINTO DE RESOLUCIÓN DE CONFLICTOS

En caso de conflicto entre los diferentes responsables, éste será resuelto por el superior jerárquico de los mismos.

5.5 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Será misión del Comité de Gestión de la Seguridad de la Información la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por el Director General en representación del Comité mediante firma y difundida para que la conozcan todas las partes afectadas.

6. DATOS DE CARÁCTER PERSONAL

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

7. GESTIÓN DE RIESGOS

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

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

Para la armonización de los análisis de riesgos, el Comité de Gestión de la Seguridad de la Información establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Gestión de la Seguridad de la Información dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

8. GESTIÓN DOCUMENTAL

Las directrices para la estructuración de la documentación del sistema, su gestión y acceso se encuentran documentadas en el procedimiento general FPA 01 Control de información documentada.

9. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política de Seguridad de la Información complementa las políticas de seguridad de Fundación EOI, F.S.P en diferentes materias:

- FPA PS01_Aspectos organizativos de la Seguridad de la Información, que establece un marco de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.
- FPA PS02_Seguridad ligada a los recursos humanos, que asegura que los empleados y contratistas entiendan sus responsabilidades y sean adecuados para desempeñar sus funciones.
- FPA PS03_Control de accesos, que define cómo limitar el acceso a los recursos de tratamiento para prevenir el acceso no autorizado, garantiza el acceso de usuarios autorizados y evitar el acceso no autorizado a los sistemas y servicios.
- FPA PS04_Cifrado, para garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información.
- FPA PS05_Seguridad física y ambiental que establece las directrices para prevenir el acceso físico no autorizado, los daños e interferencia a la información de la organización y a los recursos de tratamiento de la información.
- FPA PS06_Seguridad en las operaciones y FPA PS07_Seguridad en las Telecomunicaciones, que define las pautas a seguir para asegurar el funcionamiento correcto y seguro de las instalaciones de tratamiento de la información así como de las redes.

- FPA PS08_ Adquisición, desarrollo y mantenimiento de los Sistemas de Información, para garantizar que la seguridad de la información sea parte integral de los sistemas de información a través de todo el ciclo de vida.
- FPA PS09_ Política de Cumplimiento legal, para evitar incumplimientos de las obligaciones legales, estatutarias, reglamentarias o contractuales relativas a la seguridad de la información o de los requisitos de seguridad.
- FPA PS10_ Política de Gestión de Activos, que asegura que los empleados y contratistas entiendan sus responsabilidades y sean adecuados para desempeñar sus funciones.
- FPA P01_ Procedimiento de Gestión de riesgos de Seguridad de la Información , que define como identificar los activos de la organización y definir las responsabilidades de protección adecuadas.

La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.
La normativa de seguridad estará disponible en el repositorio documental corporativo.

10. OBLIGACIONES DEL PERSONAL

Todos los miembros de la Fundación EOI, F.S.P tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad de la Información disponer de los medios necesarios para que la información llegue a los afectados.
Todos los miembros de la Fundación EOI, F.S.P asistirán a una sesión de concienciación en materia de seguridad TIC al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de la Fundación EOI, F.S.P , en particular a los de nueva incorporación.
Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

11. TERCERAS PARTES

Cuando preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.
Cuando Fundación EOI, F.S.P utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está 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.

Firmado por Director General:

Diego Crescente de Antonio.

HISTÓRICO

Fecha de aprobación	Modificaciones
11/07/2025	Elaboración inicial del documento