POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

ender
LA FACTORÍA DE SOFTWARE

Contenido

CONTROL DE CAMBIOS

HISTÓRICO DE CAMBIOS		
VERSIÓN	**DESCRIPCIÓN DEL CAMBIO**	**FECHA DE APROBACIÓN**
1	Primera edición del documento	26/02/2024

1. Aprobación y Entrada en Vigor

Esta Política de Seguridad de la Información es efectiva desde su entrada en vigor y hasta que sea reemplazada por una nueva Política.
La Política de Seguridad será revisada por el Comité de Seguridad de la información al menos una vez al año.

2. Introducción

ENDER 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 con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, 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.

Esto implica que 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.

ENDER debe 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, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

ENDER debe estar preparado para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 8 del ENS.

2.1.Prevención

ENDER debe evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello implementará 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, van a estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, se debe:

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

2.2.Detección

Dado que los servicios se pueden 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 10 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 9 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

2.3.Respuesta

ENDER, establecerá las siguientes medidas:

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

2.4. Recuperación

Para garantizar la disponibilidad de los servicios críticos, ENDER dispondrá de planes de continuidad de los sistemas TIC como parte de su plan general de continuidad del servicio y actividades de recuperación.

3. Principios básicos

Los principios básicos son directrices fundamentales de seguridad que han de tenerse siempre presentes en cualquier actividad relacionada con el uso de los activos de información.

Se establecen los siguientes:

- **Alcance estratégico:** La seguridad de la información debe contar con el compromiso y apoyo de todos los niveles directivos de la universidad, de forma que pueda estar coordinada e integrada con el resto de las iniciativas estratégicas de la organización para conformar un todo coherente y eficaz.
- **Responsabilidad determinada**: En los sistemas TIC se identificará el Responsable de la Información, que determina los requisitos de seguridad de la información tratada; el Responsable del Servicio, que determina los requisitos de seguridad de los servicios prestados; el Responsable del Sistema, que tiene la responsabilidad sobre la prestación de los servicios y el Responsable de la Seguridad, que determina las decisiones para satisfacer los requisitos de seguridad.
- **Seguridad integral:** La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas TIC, procurando evitar cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas TIC.
- **Gestión de Riesgos:** El análisis y gestión de riesgos será parte esencial del proceso de seguridad. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales.
- **Proporcionalidad:** El establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.
- **Mejora continua:** Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado, instruido y dedicado.
- **Seguridad por defecto:** Los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.

4. Objetivos

Se han establecido los siguientes objetivos de la seguridad de la información:

- Garantizar la calidad y protección de la información.
- Lograr la plena concienciación de los usuarios respecto a la seguridad de la información.
- Gestión de activos de información: Los activos de información se encontrarán inventariados y categorizados y estarán asociados a un responsable.

- Seguridad ligada a las personas: Se implantarán los mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un su uso indebido, logrando la plena concienciación de los usuarios respecto a la seguridad de la información.
- Seguridad física: Los activos de información serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.
- Seguridad en la gestión de comunicaciones y operaciones: Se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las TIC. La información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.
- Control de acceso: Se limitará el acceso a los activos de información por parte de usuarios, procesos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo. Además, quedará registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso y auditar su uso adecuado, conforme a la actividad de la organización.
- Adquisición, desarrollo y mantenimiento de los sistemas de información: Se contemplarán los aspectos de seguridad de la información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.
- Gestión de los incidentes de seguridad: Se implantarán los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.
- Garantizar la prestación continuada de los servicios: Se implantarán los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de sus procesos de negocio, de acuerdo con las necesidades de nivel de servicio de sus usuarios.
- Protección de datos: Se adoptarán las medidas técnicas y organizativas que corresponda implantar para atender los riesgos generados por el tratamiento para cumplir la legislación de seguridad y privacidad.
- Cumplimiento: Se adoptarán las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información.

5. Alcance

Los sistemas de información que dan soporte a las actividades de:

- Desarrollo software de gestión de centros de formación Atenea
- App Atenea en la nube

6. Marco Normativo

Según la legislación vigente, las leyes aplicables a ENDER en materia de Seguridad de la Información son:

- Real Decreto 311/2022, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS).
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- Ley de Propiedad Industrial.
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de comercio electrónico.

7. Organización de la Seguridad

La implantación de la Política de Seguridad en ENDER requiere que todos los miembros de la organización entiendan sus obligaciones y responsabilidades en función del puesto desempeñado. Como parte de la Política de Seguridad de la Información, cada rol especifico, personalizado en usuarios concretos, debe entender las implicaciones de sus acciones y las responsabilidades que tiene atribuidas, quedando identificadas y detalladas en esta sección, y que se agrupan del modo siguiente:

a) El Comité de Seguridad de la Información
b) Responsable del Servicio
c) Responsable de la Información
d) Responsable de Seguridad de la Información
e) Responsable de Sistemas

En los siguientes apartados se especifican las funciones atribuidas a uno de estos roles.

7.1.Comité de seguridad de la información

El Comité de Seguridad de la Información coordina la seguridad de la información en ENDER. Dicho Comité está compuesto por cada una de las figuras anteriormente mencionadas.

Las funciones del Comité de Seguridad de la Información son las siguientes:

- Revisión y aprobación de la Política de Seguridad de la Información y de las responsabilidades principales.

- Definir e impulsar la estrategia y la planificación de la seguridad de la información proponiendo la asignación de presupuesto y los recursos precisos.
- Supervisión y control de los cambios significativos en la exposición de los activos de información a las amenazas principales, así como del desarrollo e implantación de los controles y medidas destinadas a garantizar la Seguridad de dichos activos.
- Aprobación de las iniciativas principales para mejorar la Seguridad de la Información.
- Supervisión y seguimiento de aspectos tales como:
    - Principales incidencias en la Seguridad de la Información.
    - Elaboración y actualización de planes de continuidad.
    - Cumplimiento y difusión de las Políticas de Seguridad.

El Secretario del Comité de Seguridad TIC será el Responsable de Seguridad y tendrá como funciones:

- Convocar las reuniones del Comité de Seguridad de la Información.
- Prepara los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elabora el acta de las reuniones.
- Es responsable de la ejecución directa o delegada de las decisiones del Comité.

7.2.Responsable de la Información

- Tiene la potestad de establecer los requisitos, en materia de seguridad, de la información gestionada. Si esta información incluye datos de carácter personal, además deberán tenerse en cuenta los requisitos derivados de la legislación correspondiente sobre protección de datos.
- Determina los niveles de seguridad de la información.

7.3.Responsable del Servicio

- Tiene la potestad de establecer los requisitos, en materia de seguridad, de los servicios prestados.
- Determina los niveles de seguridad de la información.

7.4.Responsable de Seguridad

Responsable de la definición, coordinación y verificación de cumplimiento de los requisitos de seguridad de la información definidos de acuerdo a los objetivos estratégicos.

Las funciones del Responsable de Seguridad de la Información son las siguientes:

- Dirigir las reuniones del Comité de Seguridad, informando, proponiendo y coordinando sus actividades y decisiones.
- Coordinar y controlar las medidas de seguridad de la información y de protección de datos de ENDER.
- Supervisar la implantación, mantener, controlar y verificar el cumplimiento de:

  - La estrategia de seguridad de la información definida por el Comité de Seguridad.
  - Las normas y procedimientos contenidos en la Política de Seguridad de la Información de ENDER y normativa de desarrollo.
- Supervisar los incidentes de seguridad producidos en ENDER.
- Difundir en ENDER las normas y procedimientos contenidos en la Política de Seguridad de la Información y normativa de desarrollo, así como las funciones y obligaciones en materia de seguridad de la información.
- Supervisar y colaborar en las Auditorías internas o externas necesarias para verificar el grado de cumplimiento de la Política de Seguridad, normativa de desarrollo y leyes aplicables en materia de protección de datos personales y de seguridad de la información.
- Asesorar en materia de seguridad de la información a las diferentes áreas operativas de ENDER.

7.5.Responsable del sistema

Es responsable de asegurar la ejecución de medidas para asegurar los activos y servicios de los sistemas de información, que soportan la actividad de ENDER, de acuerdo a los objetivos de la organización.

Las funciones del Responsable de Sistemas de la Información son las siguientes:

- Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Seleccionar y establecer las funciones y obligaciones a los Responsables Técnicos Informáticos encargados de personificar una gestión de la seguridad de los activos de ENDER, conforme a la estrategia de seguridad definida.
- Garantizar que la implantación de nuevos sistemas y de los cambios en los existentes cumple con los requerimientos de seguridad establecidos en ENDER.
- Establecer los procesos y controles de monitorización del estado de la seguridad que permitan detectar las incidencias producidas y coordinar su investigación y resolución.
- El Responsable del Sistema puede acordar la suspensión del manejo de una cierta 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 debe ser acordada con los responsables de la información afectada, del servicio afectado y el Responsable de la Seguridad, antes de ser ejecutada.

8. Procedimiento de Designación

Se designan las siguientes responsabilidades:

- Responsable del servicio y de la información:
- Responsable de seguridad:
- Responsable del sistema:

Los nombramientos se revisarán cada 2 años o cuando alguno de los puestos quede vacante.

El Responsable de Seguridad de la Información será nombrado por el Director General a propuesta del Comité de Seguridad TIC.

9. Revisión de la Política de Seguridad de la Información

Será misión del Comité de Seguridad TIC 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 y difundida para que la conozcan todas las partes afectadas.

10. Requisitos mínimos de seguridad

A continuación, se enuncian los principios básicos relacionados con la seguridad de la información, que rigen la política de seguridad de la información de la organización.

a) Organización e implantación del proceso de seguridad. Se desarrolla en el punto 6 de la presente política.
b) Análisis y gestión de los riesgos. Se desarrolla en el apartado 12 Gestión de riesgos y en el procedimiento PS.02 Planificación.
c) Gestión de personal. Se desarrolla en el apartado 16 Obligaciones del Personal y en el procedimiento PS.09 Gestión de Personal.
d) Profesionalidad. Se desarrolla en el apartado 16 Obligaciones de personal
e) Autorización y control de los accesos. El acceso del sistema de información debe ser controlado y limitado, por lo que se ha realizado un procedimiento formal de autorización, desarrollado en el procedimiento PS.01 Gestión de autorizaciones. En el apartado 19 control de accesos, se definen unas líneas básicas en la materia y se desarrolla en el procedimiento PS.03 Control de Acceso.
f) Protección de las instalaciones. Se desarrolla en el apartado 15 Seguridad Física y del entorno y en el procedimiento PS.08 Protección de instalaciones.
g) Adquisición de productos. Se desarrolla en el apartado 23 terceras partes.
h) Integridad y actualización del sistema. Todo elemento físico o lógico requerirá autorización formal previa a su instalación en el sistema por lo que se ha realizado un procedimiento formal de autorización PS.01 Gestión de autorizaciones. También se dispone de un procedimiento en el que se ha establecido como debe realizar el mantenimiento del equipamiento y la gestión de parches y vulnerabilidades.
i) Protección de la información almacenada y en tránsito. La protección de la información almacenada se desarrolla en el apartado 22 Protección de información almacenada.

Estas protecciones se desarrollan más ampliamente en el procedimiento PS.14 Protección de Información.

j) Prevención ante otros sistemas de información interconectados. Se desarrolla en el apartado 17 Gestión de comunicaciones y operaciones.
k) Registro de actividad. Se desarrolla en el apartado 18 Seguimiento y monitorización y en el procedimiento PS.04 Explotación.
l) Incidentes de seguridad. Se desarrolla en el apartado 21 Gestión de incidencias de seguridad y en el procedimiento PS.04 Explotación.
m) Mínimo privilegio. Se desarrolla en el apartado 20 Gestión de la configuración y en el procedimiento PS.04 Explotación.
n) Continuidad de la actividad. Se desarrolla en el apartado 14 Gestión de la continuidad y en el procedimiento PS.06 Continuidad del servicio.
o) Mejora continua del proceso de seguridad. Tal como se especifica en esta política, el comité del SGSI promoverá la mejora continua, de forma que se planifiquen y realicen objetivos y acciones de mejora (Apartado 7 Organización de la Seguridad) y en el procedimiento PS.00 Gestión del Sistema.

11. Datos de Carácter Personal

La Ley Orgánica de Protección de Datos (LOPD) garantiza y protege, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor, intimidad y privacidad personal y familiar, y resulta de aplicación a los datos de carácter personal registrados tanto informáticamente como en soporte papel.

Todos los sistemas de información de ENDER 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.

Para garantizar dicha protección, se adoptan las medidas de seguridad que se corresponden con las exigencias previstas en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la LOPD.

Todo usuario interno o externo que, en virtud de su actividad profesional, pudiera tener acceso a datos de carácter personal, está obligado a guardar secreto sobre los mismos, deber que se mantendrá de manera indefinida, incluso más allá de la relación laboral o profesional con ENDER.

12. 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 Seguridad TIC establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados.

El Responsable de la Seguridad será el encargado de que se realice el análisis de riesgos, así como de identificar carencias y debilidades y ponerlas en conocimiento del Comité de Seguridad de la Información.

El Comité de Seguridad TIC dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

El proceso de gestión de riesgos comprenderá las siguientes fases:

- Categorización de los sistemas.
- Análisis de riesgos.
- El Comité de Seguridad de la Información procederá a la selección de medidas de seguridad a aplicar que deberán de ser proporcionales a los riesgos y estar justificadas.

Las fases de este proceso se realizarán según lo dispuesto en los Anexos I y II del Real Decreto 311/2022, de 8 de enero, y siguiendo las normas, instrucciones, Guías CCN-STIC y recomendaciones para la aplicación del mismo elaboradas por el Centro Criptológico Nacional. En particular, para realizar el análisis de riesgos, como norma general se utilizará una metodología reconocida de análisis y gestión de riesgos.

La gestión de riesgos quedará documentada en el informe de Análisis y gestión de riesgos.

13. Desarrollo de la Política Seguridad de la Información del Personal

La presente Política de Seguridad de la Información será complementada por medio de diversa normativa y recomendaciones de seguridad (normativas y procedimientos de seguridad, procedimientos técnicos de seguridad, informes, registros y evidencias electrónicas). Corresponde al Comité de Seguridad de la Información su revisión anual y/o mantenimiento, proponiendo, en caso de que sea necesario mejoras a la misma.

El cuerpo normativo sobre seguridad de la información se desarrollará en tres niveles por ámbito de aplicación, nivel de detalle técnico y obligatoriedad de cumplimiento, de manera que cada norma de un determinado nivel de desarrollo se fundamente en las normas de nivel superior. Dichos niveles de desarrollo normativo son los siguientes:

a) Primer nivel normativo: constituido por la presente Política de Seguridad de la Información, la Normativa Interna del Uso de los Medios Electrónicos y las directrices

generales de seguridad aplicables a los organismos o unidades de la universidad a los que sea de aplicación dichos documentos.

b) Segundo nivel normativo: constituido por las normas de seguridad derivadas de las anteriores.
c) Tercer nivel normativo: constituido por procedimientos, guías e instrucciones técnicas. Son documentos que, cumpliendo con lo expuesto en la Política de Seguridad de la Información, determinan las acciones o tareas a realizar en el desempeño de un proceso.

Corresponde al órgano superior la aprobación de la Política de Seguridad de la Información y la Normativa Interna del Uso de los Medios Electrónicos de la Universidad, siendo el Comité de Seguridad de la Información el órgano responsable de la aprobación de los restantes documentos, siendo también responsable de su difusión para que la conozcan las partes afectadas.

Del mismo modo, la presente Política de Seguridad de la Información complementa la Política de Privacidad en materia de protección de datos.

La normativa de seguridad y, muy especialmente, la Política de seguridad de la Información y la Normativa Interna del Uso de los Medios Electrónicos, será conocida y estará a disposición de todos los miembros de la universidad, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones. Estará disponible para su consulta en la Intranet, en soporte papel, esta documentación será custodiada por el Servicio de Informática.

14. Gestión de la continuidad del servicio

ENDER tomará medidas para prevenir incidentes que afecten a la disponibilidad de los servicios. Se realizará un análisis de impacto y se tomarán medidas proporcionales.

Además se cuenta con un Plan de continuidad, del cual se realizan pruebas periódicas de su efectividad.

ENDER cuenta con los recursos necesarios para implementar el Plan de Continuidad.

15. Seguridad física y del entorno

Para que la seguridad lógica sea efectiva es primordial que en nuestras instalaciones se mantenga una correcta seguridad física para evitar los accesos no autorizados, así como cualquier otro tipo de daño o interferencia externa, para ello ENDER toma las precauciones necesarias para que solo las personas autorizadas tengan acceso a las instalaciones.

La totalidad de las oficinas cuentan con las barreras físicas necesarias para asegurar los recursos que éstas alberguen. Asimismo, las instalaciones de ENDER están dotadas de los dispositivos de extinción de incendios marcados por la legislación vigente en esa materia y de salidas de emergencia debidamente señalizadas.

16. Obligaciones del Personal

Todos y cada uno de los usuarios de los sistemas de información de ENDER son responsables de la seguridad de los activos de información mediante un uso correcto de los mismos, siempre de acuerdo con sus atribuciones profesionales y académicas.

Todos los miembros de ENDER 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 disponer los medios necesarios para que la información llegue a los afectados.

Los miembros de ENDER recibirán formación en seguridad de la información. Se establecerá un programa de concienciación continua para atender a todos los miembros de ENDER, 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.

El incumplimiento de la presente Política de Seguridad de la Información podrá acarrear el inicio de las medidas disciplinarias que procedan, sin perjuicio de las responsabilidades legales correspondientes.

17. Gestión de Comunicaciones y operaciones

ENDER controlará el acceso a los servicios en redes internas y externas y se asegurará de que los usuarios no ponen en riesgo dichos servicios. Para ello se han establecido las interfaces adecuadas entre la red de la organización y otras redes, los mecanismos adecuados de autenticación para usuarios y equipos, y los accesos para cada usuario del sistema de información.

Para la operación correcta y segura de los sistemas de información, existen procedimientos documentados, que deben seguirse por el personal afectado. Estos procedimientos serán revisados y convenientemente modificados cuando haya cambios significativos en los equipos o el software que así lo requieran.

18. Seguimiento y monitorización

Se definirá una estrategia global de monitorización de sistemas y actividades, identificando los sistemas más críticos y estableciendo los controles oportunos para registrar cualquier evento que debe ser detectado (actividades no autorizadas o funcionamientos inadecuados de sistemas). Los registros deberán ser almacenados convenientemente protegidos contra su modificación o eliminación.

Según se considere necesario, se establecerán los mecanismos necesarios que permitan detectar actividades de proceso de información no autorizadas. Esto implicará realizar tareas

para llevar a cabo controles e inspecciones de los registros del sistema y actividades para probar la eficiencia de la seguridad de datos y procedimientos de integridad de datos, para asegurar el cumplimiento con la política establecida y los procedimientos operativos, así como para recomendar cualquier cambio que se estime necesario.

19. Control de accesos

La información debe estar protegida contra accesos no autorizados por lo que sólo se facilitará el acceso a la información necesaria para el trabajo a desarrollar. No se permitirá el acceso a la red, a los sistemas, aplicaciones o información a ningún usuario que no esté formalmente autorizado para ello.

Cuando proveedores de servicios o empresas externas necesiten acceder a las instalaciones o la información por un motivo justificado, se requiere que firmen acuerdos de confidencialidad con la organización para mantener el mismo nivel de seguridad que si fueran empleados de la organización.

20. Gestión de la configuración

La gestión, configuración y actualización del hardware y software en los que se basan los mecanismos y servicios de seguridad del Sistema de Información se realizará siempre siguiendo los principios de seguridad por defecto y mínimo privilegio.

21. Gestión de incidencias de seguridad

Cualquier empleado que sospeche u observe una incidencia de seguridad, bien sea física (fuego, agua, etc.), de software o sistemas (virus, desaparición de datos, etc.) o de servicios de soporte (comunicaciones, electricidad, etc.) debe comunicarlo inmediatamente al Responsable de Seguridad para que tome las medidas oportunas y registre la incidencia.

Se establecerán responsabilidades y procedimientos de gestión de incidencias para asegurar una respuesta rápida, eficaz y ordenada a las incidencias en materia de seguridad. Existirán procedimientos que abarquen todos los tipos posibles de incidentes.

La operativa de este aspecto se detalla en el procedimiento “Gestión de incidentes”.

22. Protección almacenada

ENDER implantará medidas físicas y lógicas para proteger la información allí donde se encuentre almacenada, tanto si se encuentra en un soporte físico o digital. Se realizarán copias de seguridad que aseguren la posibilidad de recuperación en caso de incidente.

23. Terceras Partes

Cuando ENDER preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la Información. Se establecerán canales

para reporte y coordinación de los respectivos Comités de Seguridad TIC y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando ENDER utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte 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.

24. Estructura de la documentación de seguridad

Todos los documentos que componen la documentación del Sistema de Gestión de Seguridad de la Información se gestionarán de acuerdo a lo descrito en el procedimiento PS.00 Gestión del Sistema.

Se ha establecido un marco normativo en materia de seguridad de la información estructurado en diferentes niveles, de forma que los principios y los objetivos marcados en la política de seguridad de la institución tengan un desarrollo específico:

- Primer nivel: la presente Política de Seguridad de la Información, que debe ser aprobada por Alcaldía a propuesta del Comité de Seguridad.
- Segundo nivel: la normativa de seguridad de la información aprobada por el Comité de Seguridad de la Información en desarrollo de la Política de Seguridad de la Información. En ella se establecerán unas normas de uso aceptable de los sistemas de información Esta normativa será aprobada por el Comité de Seguridad de la Información.
- Tercer nivel: los procedimientos de seguridad de la información, en los que se detallará la manera correcta de realizar determinados procesos de modo que se proteja en todo momento la seguridad y la información. Estos procedimientos han de ser aprobados por el Responsable de Seguridad.
- Cuarto nivel: estándares de seguridad, instrucciones técnicas, buenas prácticas, recomendaciones, guías, cursos de formación, presentaciones, etc. Ha de ser aprobada por el Responsable de Seguridad.

Los documentos que integran el Sistema de Gestión de Seguridad de la Información se encuentran, en soporte digital, a disposición de todo el personal al que le sea necesario para el desempeño de las funciones relacionadas con su puesto de trabajo. Estará disponible para su consulta, sin posibilidad de modificación.

Firmado: Jonathan Estrella Fernández

Responsable de la Información y del Servicio