Política de Seguridad de la Información (ENS)

Control de versiones:

Astron informática y comunicaciones	**POLÍTICA DE SEGURIDAD**	FECHA:1/09/2024 REV.0

IDENTIFICACIÓN	
POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Revisión: 0
Ámbito: FOMENTO DE TÉCNICAS EXTREMEÑAS	Estado: Aprobada

REGISTRO DE CAMBIOS			
Revisión	Cambio	Apartado	Fecha
0	Elaboración del documento inicial	Todos	1/09/2024

Aprobado por: Comité de Seguridad
Fecha de aprobación: 1 de septiembre de 2024

Astron informática y comunicaciones	**POLÍTICA DE SEGURIDAD**	FECHA:1/09/2024 REV.0

1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado por la Gerencia de ***Fomento de Técnicas Extremeñas***, el día 9 de septiembre de 2021. Esta Política de Seguridad de la Información es efectiva desde dicha fecha y estará vigente hasta que sea reemplazada por una nueva.

La entrada en vigor de la presente Política de Seguridad de la Información supone la derogación de cualquier otra que existiera a cualquier nivel de la organización.

2. INTRODUCCIÓN

Fomento de Técnicas Extremeñas 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 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.
Esto implica que se deben aplicar las medidas de seguridad exigidas por el Esquema Nacional de Seguridad y la Ley Orgánica de Protección de Datos y Reglamento Europeo de Protección de Datos, 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.

Fomento de Técnicas Extremeñas debe cerciorarse de que la seguridad de la información 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.

Fomento de Técnicas Extremeñas debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Esquema Nacional de Seguridad y a la Ley Orgánica de Protección de Datos.

Esta Política de Seguridad sigue las indicaciones de la ***guía CCN-STIC-805*** del Centro Criptológico Nacional, centro adscrito al Centro Nacional de Inteligencia.

2.1. PREVENCIÓN

Fomento de Técnicas Extremeñas 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 se implementarán las medidas mínimas de seguridad determinadas por el ENS, RGPD y la LOPD, 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, ***Fomento de Técnicas Extremeñas*** 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, es preciso 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, tanto regularmente, como cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

2.3. RESPUESTA

Fomento de Técnicas Extremeñas establecerá las siguientes medidas:

- Mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecerá protocolos de intercambio de información sobre posibles incidentes con clientes y proveedores.

2.4. RECUPERACIÓN

Para garantizar la disponibilidad de los servicios y la resiliencia de sus sistemas de información, ***Fomento de Técnicas Extremeñas*** dispone de los medios y técnicas necesarios que permiten garantizar la recuperación de los servicios esenciales.

3. ALCANCE

Esta Política de seguridad de la información se aplicará a los sistemas de información de ***Fomento de Técnicas Extremeñas*** relacionados con el ejercicio de sus competencias y a todos los usuarios con acceso autorizado a los mismos con independencia de la naturaleza de su relación jurídica con la organización. Todos ellos tienen la obligación de conocer y cumplir esta Política y la normativa de seguridad derivada, siendo responsabilidad del Comité de seguridad de la información disponer los medios necesarios para que la información llegue al personal afectado.

4. MISIÓN

Fomento de Técnicas Extremeñas define la presente Política de Seguridad de la Información, de carácter obligatorio para empleados y empresas colaboradoras, teniendo como objetivo fundamental garantizar la seguridad de la información y la prestación continuada de los servicios que proporciona, actuando preventivamente, supervisando la actividad y reaccionando con celeridad frente a los incidentes que puedan ocurrir.

Esta Política debe sentar las bases para que el acceso, uso, custodia y salvaguarda de los activos de información, de los que se sirve ***Fomento de Técnicas Extremeñas*** para desarrollar sus funciones, se realicen, bajo garantías de seguridad, en sus distintas dimensiones:

- **Disponibilidad:** propiedad o característica de los activos consistentes en que las entidades o procesos autorizados tengan acceso a los mismos cuando lo requieran.
- **Integridad:** propiedad o característica consistente en que el activo de información no sea alterado de manera no autorizada.
- **Confidencialidad:** propiedad o característica consistente en que la información ni se ponga a disposición, ni se revele a individuos, entidades o procesos no autorizados.
- **Autenticidad:** propiedad o característica consistente en que una entidad sea quien dice ser o bien que garantice la fuente de la que proceden los datos.
- **Trazabilidad:** propiedad o característica consistente en que las actuaciones de una entidad puedan ser imputadas exclusivamente a dicha entidad.

Bajo estas premisas los objetivos específicos de la Seguridad de la información en ***Fomento de Técnicas Extremeñas*** serán:

- Velar por la seguridad de la información, en las distintas dimensiones antes descritas.
- Gestionar formalmente la seguridad, sobre la base de procesos de análisis de riesgos.
- Elaborar, mantener y probar los planes de contingencias y continuidad de la actividad que se definan para los distintos servicios ofrecidos por la organización.
- Realizar una adecuada gestión de incidencias que afecten a la seguridad de la información.
- Mantener informado a todo el personal acerca de los requerimientos de seguridad, y difundir buenas prácticas para el manejo seguro de la información.
- Proporcionar los niveles de seguridad acordados con terceras partes cuando se compartan o cedan activos de información.
- Cumplir con la reglamentación y normativa vigente.

Está Política de Seguridad:

- Se aprobará formalmente por la organización.
- Se revisará regularmente, de manera que se adapte a las nuevas circunstancias, técnicas u organizativas, y evite la obsolescencia.
- Se comunicará a todos los empleados y empresas externas qué trabajen con ***Fomento de Técnicas Extremeñas***.

5. MARCO NORMATIVO

La organización ha creado un repositorio de normativa y requisitos legales, que actualiza de forma periódica y que está disponible en la nube privada de la organización.

6. ORGANIZACIÓN DE LA SEGURIDAD

6.1. COMITÉS: FUNCIONES Y RESPONSABILIDADES

El Comité de Seguridad coordina la seguridad de la información en ***Fomento de Técnicas Extremeñas***. Este Comité dará soporte a la organización y estará formado por:

- Responsable del Servicio
- Responsable de la Información
- Responsable de Seguridad
- Responsable del Sistema

El **Comité de Seguridad** tendrá las siguientes funciones:

- Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información.
- Elaborar la estrategia de evolución de ***Fomento de Técnicas Extremeñas*** en lo que respecta a seguridad de la información.

- Elaborar y revisar regularmente la Política de Seguridad de la Información para que sea aprobada por la organización.
- Aprobar la normativa de seguridad de la información.
- Elaborar y aprobar los requisitos de formación y calificación de los Responsables de área, técnicos y usuarios desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por ***Fomento de Técnicas Extremeñas*** y recomendar posibles actuaciones respecto de ellos.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones al respecto. En particular, velar por la coordinación de los diferentes departamentos en la gestión de incidentes de seguridad de la información.
- Promover la realización de auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Aprobar planes de mejora de la seguridad de la información para ***Fomento de Técnicas Extremeñas***.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular, deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- Informar regularmente del estado de la seguridad de la información a la Dirección.

6.2. ROLES: FUNCIONES Y RESPONSABILIDADES

Serán funciones y responsabilidades del **Responsable del Servicio**:

- Establecer los requisitos del servicio en materia de seguridad, incluyendo los requisitos de interoperabilidad, accesibilidad y disponibilidad.
- Determinar los niveles de seguridad de los servicios.
- Aprobar formalmente el nivel de seguridad del servicio.

Serán funciones y responsabilidades del **Responsable de la Información:**

- Velar por el buen uso de la información y, por tanto, de su protección.
- Ser responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.

- Establecer los requisitos de la información en materia de seguridad.
- Determinar los niveles de seguridad de la información.
- Aprobar formalmente el nivel de seguridad de la información.

Serán funciones y responsabilidades del **Responsable de Seguridad:**

- Mantener el nivel adecuado de seguridad de la información manejada y de los servicios prestados por los sistemas.
- Realizar o promover las auditorías periódicas a las que obliga el ENS para verificar el cumplimiento de los requisitos del mismo.
- Gestionar la formación y concienciación en materia de seguridad TIC.
- Comprobar que las medidas de seguridad existentes son las adecuadas para las necesidades de la entidad.
- Revisar, completar y aprobar toda la documentación relacionada con la seguridad del sistema.
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría implementados en el sistema.
- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución, emitiendo informes periódicos sobre los más relevantes al Comité.

Responsable del Sistema:

- Gestionar el Sistema de Información durante todo su ciclo de vida, desde la especificación, instalación hasta el seguimiento de su funcionamiento.
- Definir los criterios de uso y los servicios disponibles en el Sistema.
- Definir las políticas de acceso de usuarios al Sistema.
- Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema.
- Determinar la configuración autorizada de hardware y software a utilizar en el Sistema y aprobar las modificaciones importantes de dicha configuración.
- Realizar el análisis y gestión de riesgos en el Sistema.
- Elaborar y aprobar la documentación de seguridad del Sistema.
- 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.
- Implantar y controlar las medidas específicas de seguridad del Sistema.
- Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.
- Suspensión del manejo de cierta información o la prestación de un cierto servicio si detecta deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos.

6.3. PROCEDIMIENTOS DE DESIGNACIÓN

La Dirección asigna, renueva y comunica las responsabilidades, autoridades y roles en lo referente a la seguridad de la información, determinando en cada caso los motivos y el plazo de vigencia. También se asegurará de que los usuarios conocen, asumen y ejercen las responsabilidades, autoridades y roles asignados, resolviendo los conflictos que se generen en relación con cada responsabilidad en Seguridad de la Información.

El responsable de la seguridad será distinto del responsable del sistema, no debiendo existir dependencia jerárquica entre ambos.

6.4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

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

7. DATOS DE CARÁCTER PERSONAL

La organización sólo recogerá datos de carácter personal cuando sean adecuados, pertinentes y no excesivos, y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido. De igual modo, adoptará las medidas de índole técnica y organizativas necesarias para el cumplimiento de la normativa de Protección de Datos vigente en cada caso.

De igual forma, con la LOPDGDD se han adaptado las medidas oportunas tales como, el análisis de legitimidad jurídica de cada uno de los tratamientos de datos que se lleven a cabo, el análisis de riesgos, la evaluación de impacto si el riesgo es alto, el registro de actividades y el encargado de desempeñar las funciones relacionadas con dicha Protección de Datos.

8. 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 establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes

servicios prestados. El Comité de Seguridad dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.
La gestión de riesgos quedará documentada en el informe de activos y evaluación de riesgos de la organización.

9. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La presente Política de seguridad de la información será complementada por medio de diversa normativa y recomendaciones de seguridad (normativas, procedimientos técnicos de seguridad, informes, registros y evidencias electrónicas). Corresponde al Comité de seguridad de la información su revisión anual y mantenimiento, proponiendo mejoras cuando sea necesario.

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 fundamenta en las normas de nivel superior. Dichos niveles de desarrollo normativo son los siguientes:

- 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 organización a los que sean de aplicación dichos documentos.
- Segundo nivel normativo: constituido por las normas de seguridad derivadas de las anteriores
- 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.

Cuando resulte procedente, se deberá recabar la opinión de los usuarios, tanto internos como externos, sin perjuicio de que se adopten las medidas necesarias para proteger los intereses y el buen funcionamiento de la organización.

10. OBLIGACIONES DEL PERSONAL

Todos los miembros de ***Fomento de Técnicas Extremeñas*** tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de ***Fomento de Técnicas Extremeñas*** recibirán concienciación en materia de seguridad al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de ***Fomento de Técnicas Extremeñas***, 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 como si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

11. TERCERAS PARTES

Cuando ***Fomento de Técnicas Extremeñas*** preste servicios a otras organizaciones o maneje su información, se les hará partícipes de esta Política de seguridad de la información. Se establecerán canales para el reporte y la coordinación de los respectivos comités de seguridad de la información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando ***Fomento de Técnicas Extremeñas*** utilice servicios de terceros o les ceda información, se les hará partícipes de esta Política de seguridad y de la normativa de seguridad que afecte a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en esta 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 estos terceros esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política de seguridad.

Cuando algún aspecto de esta Política de seguridad de la información no pueda ser satisfecho por una tercera parte, según se requiere en los párrafos anteriores, se precisará de un informe del responsable de seguridad que notifique los riesgos en que se incurre y la forma de tratarlos, que se remitirá al Comité de seguridad de la información para su evaluación y toma de decisiones.