POLÍTICA DE SEGURIDAD ENS

05264367N EDUARDO QUINTERO (R:A11029279)

Firmado digitalmente por 05264367N EDUARDO QUINTERO (R:A11029279)
Fecha: 2024.11.07 12:57:26 +01'00'

REGISTRO DE EDICIONES

Edición	Fecha	Descripción del cambio
1.0	31/05/2016	Redacción inicial.
1.1	01/04/2019	Cambios en la codificación de los documentos
1.2	01/01/2020	Cambios como consecuencia auditoría interna: roles y responsabilidades. Quitar a CV del alcance.
1.3	10/06/2020	Modificación para incluir todos los requisitos ENS según la guía CCN-STIC-805 como consecuencia de NC de auditoría externa 2020.
1.4	30/11/2023	Actualización del formato del documento. Adecuación ENS RD 311 / 2022 Se añade medida compensatoria MC03 por el requisito de independencia jerárquica entre el Responsable de Seguridad y los Responsables de los Sistemas
1.5	07/11/2024	Se incluye misión, visión y valores (OBS-01 AINT (27001 - ENS)).

Contenido

1 OBJETO 4

2 ÁMBITO DE APLICACIÓN 4

3 DOCUMENTACIÓN RELACIONADA 5

4 DEFINICIONES 5

5 ACTIVIDADES 5

5.1 OBJETIVOS Y MISIÓN 5

5.2 MARCO LEGAL Y REGULATORIO EN EL QUE SE DESARROLLAN LAS ACTIVIDADES 6

5.3 ORGANIZACIÓN DE LA SEGURIDAD 7

5.3.1 MECANISMOS DE COORDINACIÓN Y COMITÉS 7

5.3.2 FUNCIONES Y RESPONSABILIDADES DE SEGURIDAD 7

5.3.3 DESIGNACIÓN DE FUNCIONES 9

5.3.4 RESOLUCIÓN DE CONFLICTOS 9

5.4 CONCIENCIACIÓN Y FORMACIÓN 10

5.5 GESTIÓN DE RIESGOS 10

5.6 DATOS DE CARÁCTER PERSONAL 10

5.7 DETERMINACIÓN DE LA CATEGORÍA Y DEL NIVEL DE SEGURIDAD REQUERIDO PARA LOS SISTEMAS 10

5.8 DOCUMENTACIÓN. 12

5.9 ESTABLECIMIENTO, IMPLANTACIÓN, MANTENIMIENTO Y MEJORA DEL SGSI Y DIRECTRICES PARA LA GESTIÓN DE LA DOCUMENTACIÓN 12

6 FORMATOS 16

7 REGISTROS 16

1 OBJETO

La Dirección Ejecutiva de Signe, en el marco de su competencia general e indelegable de determinar las políticas y estrategias generales de la organización, y siguiendo las directrices definidas en la Política de Seguridad de la Información, aprueba la siguiente Política de Seguridad ENS aplicable a todo el Grupo Signe.

El objetivo de esta Política es definir y establecer los principios, criterios y objetivos de mejora que rigen las actuaciones en materia de seguridad de la información de los sistemas del Grupo Signe que se encuentran sujetos al Sistema de Gestión de Seguridad de la información (en adelante, SGSI) y en el alcance del Esquema Nacional de Seguridad (ENS).

En concreto, establecer las directrices y principios que regirán el modo en que las sociedades del Grupo Signe gestionarán y protegerán su información y sus servicios, cumpliendo con los objetivos y directrices de la Política de Seguridad de la Información corporativa, a través de la implantación, mantenimiento y mejora de un SGSI y aplicando los requisitos y medidas de seguridad dentro del marco regulatorio legal y vigente como el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, que exige el establecimiento de los principios y requisitos de una política de seguridad en la utilización de medios electrónicos que permita la adecuada protección de la información.

2 ÁMBITO DE APLICACIÓN

Tomando en cuenta el contexto en el cual se determinan las cuestiones internas y externas de la organización, las partes interesadas que son relevantes y sus requisitos para la seguridad de la información, así como las interfaces y dependencias entre las actividades realizadas por la entidad y las que se llevan a cabo por otras organizaciones en el cumplimiento. Esta Política se circunscribe a los servicios y sistemas de las sociedades del Grupo Signe incluidos en el alcance del SGSI que da cobertura al cumplimiento de los requisitos y medidas de seguridad establecidas en el Esquema Nacional de Seguridad.

Estos servicios incluidos dentro del ENS son los siguientes:

"Los sistemas de información soporte de las actividades de:

- Emisión de documentos en formato electrónico y
- Prestación de servicios de confianza para las actividades de:
  - Creación, verificación y validación de firmas electrónicas,
  - Sellos electrónicos o sellos de tiempo electrónicos,
  - Servicios de entrega electrónica certificada,
  - Certificados relativos a estos servicios.
    - Emisión de certificados electrónicos de diferentes perfiles según las políticas de certificados.
    - Gestión de certificados electrónicos en la nube."

con relación al documento de categorización vigente".

Estas actividades se realizan desde las instalaciones del Grupo ubicadas en:

- Oficinas Tres Cantos: Avda. de la Industria, 18, 28760 Tres Cantos, Madrid.

3 DOCUMENTACIÓN RELACIONADA

GSIGNE-GRAL-MSG Manual de Sistemas de Gestión

4 DEFINICIONES

No aplican.

5 ACTIVIDADES

5.1 OBJETIVOS Y MISIÓN

Nuestra MISIÓN: Ser una empresa familiar, líder en seguridad documental y nuevas tecnologías, caracterizada por la aplicación de los máximos estándares de calidad e innovación tecnológica en sus productos y servicios, para la consecución de sus objetivos empresariales.

Nuestra VISIÓN: Generar confianza a nuestros clientes, trabajadores y accionistas mediante productos y servicios de seguridad documental y tecnológica prestados en base a los valores corporativos.

Nuestros VALORES: Honestidad, confianza y transparencia, calidad y eficiencia, Responsabilidad Social, solidaridad intergeneracional

Mediante esta Política el Grupo Signe asume y promueve los siguientes principios generales que deben guiar todas sus actividades:

a) Garantizar el cumplimiento con los objetivos y principios generales detallados en la Política de Seguridad de la Información aprobada y promovida por la Dirección Ejecutiva.
b) Asegurar el establecimiento y cumplimiento de la presente Política y los objetivos de la seguridad de la información, y que estos sean compatibles con la estrategia de las empresas del Grupo Signe.
c) Asegurar la integración y el cumplimiento de los requisitos aplicables del SGSI/ENS en los servicios y procesos de la sociedad.
d) Asegurar que los recursos necesarios para el SGSI/ENS estén disponibles.
e) Comunicar la importancia de una gestión de la seguridad eficaz y conforme con los requisitos del SGSI/ENS.
f) Asegurar que el SGSI/ENS consigue los resultados previstos.
g) Dirigir y apoyar a las personas para contribuir a la eficacia del SGSI/ENS.
h) Promover la mejora continua.
i) Asegurar la vigilancia continua.

j) Realización de reevaluaciones periódicas.
k) Apoyar otros roles pertinentes de la Dirección, liderando a sus áreas de responsabilidad en seguridad de la información.

Los objetivos de seguridad de la información se establecerán en las funciones y niveles pertinentes, enfocados a la mejora y utilizando como marco de referencia:

a) Cambios en las necesidades de las partes interesadas que lleven a una mejora del alcance del sistema.
b) Requisitos de seguridad de la información aplicables y los resultados de la apreciación y del tratamiento de los riesgos para garantizar la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información, así como la protección de los datos personales.
c) Factores internos como la aplicación de técnicas organizativas que mejoren el seguimiento de la tramitación y resolución de incidentes de seguridad.
d) Factores externos como los avances tecnológicos, cuya aplicación mejoren la eficacia del tratamiento de los riesgos.
e) La mejora de la eficacia de la formación y concienciación del personal que trabaja en la entidad y afecta a su desempeño en seguridad de la información.

Así mismo, la planificación para la consecución de los objetivos de seguridad de la información establecidos se realizará tomando en cuenta lo que se va a hacer, los recursos necesarios, el responsable y el plazo de consecución.

5.2 MARCO LEGAL Y REGULATORIO EN EL QUE SE DESARROLLAN LAS ACTIVIDADES

a) Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
b) Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.
c) 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.
d) 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).
e) Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
f) El SGSI del Grupo Signe se mantendrá cumpliendo y respetando la Ley de Propiedad Intelectual en lo que se refiere al uso del software, obteniendo las licencias

correspondientes y llevando un registro y control de estas para el empleo adecuado de éstas en el desarrollo de las actividades.

El Grupo SIGNE dispone de un registro de legislación aplicable en el que se identifica toda la legislación en materia de seguridad de la información y su adecuación y cumplimiento en la empresa.

5.3 ORGANIZACIÓN DE LA SEGURIDAD

La Dirección del Grupo Signe tiene como responsabilidad fundamental la de liderar y comprometerse con respecto al Sistema de Gestión.

5.3.1 MECANISMOS DE COORDINACIÓN Y COMITÉS

Se designa como órgano responsable del sistema al Comité de Sistemas de Gestión que dispone de las siguientes funciones:

- Elaborar la Política de Seguridad de la Información
- Asegurarse de que se establecen, implementan y mantienen los procesos necesarios para el SGSI.
- Aprobar los procedimientos de seguridad de la información
- Realizar el seguimiento de los procesos de gestión de los incidentes de seguridad y recomendar acciones de mejora
- Velar porque la seguridad de la información se tenga en cuenta desde las fases iniciales de los proyectos hasta su puesta en operación
- Informar regularmente a la Dirección del estado de la seguridad de la información
- Asegurarse de que se promueva la toma de conciencia de los requisitos del cliente y resto de Partes Interesadas en todos los niveles de la organización.

La composición del Comité de Sistemas de Gestión y su relación con el resto de los elementos de la organización está recogida en el GSIGNE-RRHH-PR-01 Funciones y Responsabilidades.

5.3.2 FUNCIONES Y RESPONSABILIDADES DE SEGURIDAD

- Responsable de la información:
  - Determina los requisitos de la información tratada en materia de seguridad,
  - Tiene la responsabilidad última del uso que se haga de la información y, por tanto, de su protección.
  - Es el responsable último de cualquier error o negligencia que conlleve un incidente de confidencialidad o de integridad (en materia de protección de datos) y de disponibilidad (en materia de seguridad de la información).
  - El ENS asigna al Responsable de la Información la potestad de establecer los requisitos y los niveles de seguridad necesarios para la información en materia de seguridad.
  - El Responsable de la Información es el responsable de determinar la valoración del sistema y de su aprobación

- Del mismo modo, deberá de proponer el nivel de riesgo aceptable y aprobar el análisis de riesgos.

- Responsable del servicio:
  - Determina los requisitos de los servicios prestados.
  - El ENS asigna al Responsable del Servicio la potestad de establecer los requisitos del servicio en materia de seguridad. O, en terminología del ENS, la potestad de determinar los niveles de seguridad de los servicios, pudiendo ser una persona física concreta o un órgano colegiado.
  - El Responsable del Servicio también deberá aprobar el documento de Valoración del Sistema y el Análisis de Riesgos.

- Responsable de Seguridad:
  - Determina las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos por los responsables de la información y de los servicios.
  - Determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisa la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones.
  - El Responsable de Seguridad determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.
  - Aprobación de la Declaración de Aplicabilidad.
  - Aprobación del Análisis de Riesgos.

- Responsable del Sistema:
  - Por sí o a través de recursos propios o contratados, se encargará de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad
  - Se encarga de la operación del sistema de información, atendiendo a las medidas de seguridad determinadas por el Responsable de Seguridad. Su responsabilidad puede estar situada dentro de la organización (utilización de sistemas propios) o estar compartimentada entre una responsabilidad mediata (de la propia organización) y una responsabilidad inmediata (de terceros, públicos o privados), cuando los sistemas de información se encuentran externalizados.
  - Los informes de autoevaluación y/o los informes de auditoría serán analizados por el Responsable de Seguridad, que elevará las conclusiones al Responsable del Sistema para que adopte las medidas correctoras adecuadas.
  - En los casos excepcionales en los que exista una dependencia jerárquica del Responsable del Seguridad sobre el Responsable del Sistema, este último no podrá recibir instrucciones respecto al desempeño de sus funciones como Responsable del Sistema, debiendo responder directamente al más alto nivel jerárquico.

- POC (Punto o Persona de Contacto) para la seguridad de la información tratada y el servicio prestado, cuenta con el apoyo de los órganos de dirección, y canaliza y supervisa, tanto el cumplimiento de los requisitos de seguridad del servicio que presta o solución que provea, como las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dicho servicio. El POC de seguridad es el propio Responsable de Seguridad de la organización y formará parte del Área de Sistemas de la Información. Todo ello sin perjuicio de que la responsabilidad última resida en la entidad del sector público destinataria de los citados servicios.

- Administrador del sistema: Cumplimiento de los procedimientos técnicos de seguridad de la información.
  - Velar por el cumplimiento de las políticas de seguridad.

- Administradores funcionales de aplicaciones: Altas, bajas y gestión de privilegios en las aplicaciones.

- Delegado de Protección de Datos (DPO) y Responsable de Privacidad: Velar por el cumplimiento de los requisitos en materia de protección de datos de carácter personal.

5.3.3 DESIGNACIÓN DE FUNCIONES

La Dirección asegura, con la colaboración del RSGSI, que el personal dispone de la necesaria formación teórica y práctica en materia de seguridad de la información para el desempeño eficiente de sus funciones.

Las funciones y responsabilidades inherentes a cada puesto de trabajo dentro del SGSI, así como los requisitos de formación y experiencia necesarios, están recogidas en los perfiles de puesto de trabajo.

Las modificaciones de los roles y funciones de seguridad serán aprobados por la dirección del Grupo Signe.

5.3.4 RESOLUCIÓN DE CONFLICTOS

La resolución de conflictos correrá a cargo de la Dirección.

5.4 CONCIENCIACIÓN Y FORMACIÓN

Dentro de los planes de formación se incluirán acciones de concienciación orientadas al personal de forma que se realice una concienciación relativa, entre otros, a los siguientes aspectos:

- Política de seguridad de la información.
- Seguridad de la información.
- Riesgos, vulnerabilidades y amenazas de los sistemas de información.
- Necesidad del cumplimiento de la legislación vigente

5.5 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 Sistemas de Gestión establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Sistemas de Gestión dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

5.6 DATOS DE CARÁCTER PERSONAL

El tratamiento de datos de carácter personal se basará en la "SIGNE-RGPD-POL-01 Politica protección datos personales", en la que se fijan las directrices que se deben seguir en el Grupo para garantizar la privacidad de los datos de los clientes, proveedores, empleados y, en general, de todos los colectivos de datos implicados, identificando la base de legitimación más adecuada para los tratamientos de datos personales llevados a cabo de acuerdo con la legislación vigente.

5.7 DETERMINACIÓN DE LA CATEGORÍA Y DEL NIVEL DE SEGURIDAD REQUERIDO PARA LOS SISTEMAS

La categoría en materia de seguridad, de los sistemas de información en el alcance del Esquema Nacional de Seguridad, se determinará en función de la valoración del impacto que tendría un incidente que afecte a la seguridad de la información o de los servicios con perjuicio para la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad.

La valoración de las consecuencias del impacto se efectuará atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los ciudadanos.

La facultad para determinar la categoría de un sistema le corresponde al responsable del servicio y al responsable de la información; y será de aplicación a todos los sistemas empleados para la prestación de los servicios incluidos en el alcance del Esquema Nacional de Seguridad.

El proceso de categorización de los sistemas se realizará a través de las siguientes actividades:

- Identificación del nivel correspondiente a cada servicio/información, en función de las dimensiones de seguridad.
- Determinación de la categoría del sistema, teniendo en cuenta que cuando un sistema maneja diferentes informaciones y presta diferentes servicios, el nivel del sistema en cada dimensión, será el mayor de los establecidos para cada información y servicios.

La identificación del nivel correspondiente a cada servicio/información en las dimensiones disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad se realizará considerando los siguientes criterios definidos en el Esquema Nacional de Seguridad:

- Nivel BAJO (B). Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio limitado sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.
- Nivel MEDIO (M). Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.
- Nivel ALTO (A). Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio muy grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

La clasificación se realizará en base a las siguientes categorías: BÁSICA (B), MEDIA (M) y ALTA (A).

- Un sistema de información será de categoría ALTA (A) si alguna de sus dimensiones de seguridad alcanza el nivel ALTO (A).
- Un sistema de información será de categoría MEDIA (M) si alguna de sus dimensiones de seguridad alcanza el nivel MEDIO (M), y ninguna alcanza un nivel superior.

- Un sistema de información será de categoría BÁSICA (B) si alguna de sus dimensiones de seguridad alcanza el nivel BAJO (B), y ninguna alcanza un nivel superior.

La calificación de la información será realizada por el responsable de la información considerando lo establecido legalmente sobre la naturaleza de la misma. Los responsables de la información y de cada servicio serán designados por la dirección y se identificarán en el documento de "GSIGNE-RRHH-PR-01-F02 Listado de puestos de trabajo vs personas".

La valoración del sistema de información y la determinación de la categoría del sistema será documentada en la Declaración de Aplicabilidad, siendo el responsable de la información y del servicio el responsable de su documentación y aprobación formal. Además, en cada momento tendrá en exclusiva la potestad de modificar el nivel de seguridad requerido, de acuerdo a los criterios descritos en el presente documento.

Considerando la categoría del sistema y los niveles asociados a cada dimensión de seguridad, se determinarán las medidas que se deberán aplicar a dicho sistema.

5.8 DOCUMENTACIÓN.

La información documentada asociada al ENS se organiza, codifica y aprueba de acuerdo con los requisitos generales del Sistema de Gestión del Grupo Signe que se recogen en el documento "GSIGNE-GRAL-MSG Manual de Sistemas de Gestion".

Toda la información documentada relativa a los Sistemas de Gestión, incluido el tratamiento del ENS se aloja en los Sistemas de Información del Grupo Signe.

5.9 ESTABLECIMIENTO, IMPLANTACIÓN, MANTENIMIENTO Y MEJORA DEL SGSI Y DIRECTRICES PARA LA GESTIÓN DE LA DOCUMENTACIÓN

Los controles de seguridad deberán implantarse, mantenerse y mejorarse continuamente, y estar disponibles como información documentada que deberá ser revisada y aprobada por la dirección.

En cumplimiento del artículo 12 del Real Decreto del ENS, la presente Política de Seguridad se desarrollará aplicando los siguientes requisitos mínimos que se encuentran incluidos en la documentación del sistema:

a) Organización e implantación del proceso de seguridad.

   Considerando las directrices desarrolladas en la Política de Seguridad de la Información y en la Política de Seguridad del ENS, se desarrollarán un conjunto de procedimientos operativos que permitan garantizar la implantación de dichas directrices, y la consecución de los objetivos de la organización en materia de seguridad de la información.

b) Análisis y gestión de los riesgos.

El proceso de análisis y gestión de los riesgos se realizará de acuerdo con las siguientes actividades:

- Identificación de activos.
- Análisis y valoración.
- Cálculo del riesgo.
- Determinación del riesgo aceptable.

El desarrollo de estas actividades se encuentra recogido en la metodología de análisis de riesgos.

c) Gestión de personal.

La Dirección se asegurará que el personal dispone de la formación necesaria teórica y práctica en materia de seguridad de la información para el desempeño eficiente de sus funciones.

Para lograr los objetivos de seguridad de la información todo el personal debe estar involucrado en el tratamiento y saber de qué forma se puede contribuir a su consecución.

Estas medidas se encuentran desarrolladas en el procedimiento de seguridad relativa a los recursos humanos.

d) Profesionalidad.

La Dirección deberá garantizar que el personal dispone del conocimiento y habilidades necesarias para el adecuado desempeño de sus funciones. Además, deberá proporcionar la formación necesaria cuando se detecten carencias en el cumplimiento de las actividades.

e) Autorización y control de los accesos.

Los sistemas de información deberán disponer de un mecanismo de control de accesos que limite su acceso a los usuarios y dispositivos que estén debidamente autorizados, restringiendo el acceso a las funciones que le son permitidas.

Las medidas de seguridad aplicadas se encuentran descritas en el procedimiento de control de acceso.

f) Protección de las instalaciones.

La organización deberá disponer de un conjunto de controles de acceso físico a las instalaciones, que permita limitar el acceso únicamente a las personas autorizadas a las zonas de almacenamiento y/o procesamiento de información confidencial.

Las medidas de protección se encuentran descritas en el procedimiento de seguridad física y del entorno.

g) Adquisición de productos de seguridad y contratación de servicios de seguridad.

La adquisición de productos y servicios deberá considerar y garantizar el cumplimiento con los requisitos de seguridad establecidos por la Dirección, tal y como se detalla en el procedimiento de adquisición, desarrollo y mantenimiento.

h) Mínimo privilegio.

Los sistemas deberán configurarse según las políticas y procedimientos de seguridad definidos. El procedimiento de seguridad de las operaciones desarrolla las medidas de seguridad que se deben aplicar a los sistemas de información en el que se considera siempre el principio de mínimo privilegio.

i) Integridad y actualización del sistema.

Se deberán aplicar medidas que permitan conocer el estado de seguridad de los sistemas, y que permitan identificar y gestionar los riesgos de seguridad de los mismos. Estas medidas se encuentran desarrolladas en el procedimiento de seguridad de las operaciones.

j) Protección de la información almacenada y en tránsito.

Se deberán aplicar medidas de seguridad que permitan garantizar un adecuado nivel de protección de la información almacenada y en tránsito. Estas medidas se encuentran detalladas en el procedimiento de gestión de activos.

k) Prevención ante otros sistemas de información interconectados.

Se deberán analizar y gestionar los riesgos derivados de las conexiones de los sistemas de información con redes públicas, y aplicar las medidas necesarias de protección según el nivel de seguridad requerido por el sistema.

l) Registro de actividad y detección de código dañino.

Los sistemas de información deberán contar con registros de actividad de los usuarios que permitan custodiar la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas. Además, se deberá disponer de sistemas que permitan la detección de código dañino

m) Incidentes de seguridad.

Los sistemas de información deberán contar con un sistema de detección y reacción frente a código dañino. Además, existirá un registro de incidentes de seguridad que permitirá realizar un seguimiento de la resolución de los mismos y aplicar mejoras a través de las lecciones aprendidas.

n) Continuidad de la actividad.

Se deberán establecer, en la medida de lo posible y según el nivel de riesgo asociado, los mecanismos necesarios para garantizar la recuperación de la información y la continuidad de las operaciones.

o) Mejora continua del proceso de seguridad.

La Dirección deberá llevar a cabo una revisión periódica del sistema para asegurarse de su conveniencia, adecuación y eficacia continua. Ante la ocurrencia de cualquier

desviación respecto a los resultados esperados, se deberá iniciar el proceso de tratamiento de la misma mediante los procesos establecidos.

Esta Política se desarrollará por medio de normativa y procedimientos de seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización dentro del alcance que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

Se deberá comunicar la información documentada de los controles de seguridad al personal que trabaja en la entidad (personal interno y externo), que tendrá la obligación de aplicarla en la realización de sus actividades laborales.

La información documentada será clasificada en: información de uso público, información de uso interno e información confidencial, dando el uso adecuado de acuerdo con dicha clasificación y según el criterio que se establezca en la Política de Gestión de Activos.

Esta Política de Seguridad del ENS ha sido aprobada y revisada, por última vez, por la Dirección General Corporativa.

6 FORMATOS

N/A

7 REGISTROS

IDENTIFICACIÓN	SOPORTE	RESPONSABLE	ARCHIVO	TIEMPO DE CONSERVACIÓN
N/A	N/A	N/A	N/A	N/A