# POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN ENS

La Dirección de **Esvora**, consciente de la necesidad de promover, mantener y mejorar el enfoque hacia el cliente en todas sus actividades, ha implantado un GRC (Gestión Riesgo y Cumplimiento) conforme al estándar cuyo **objetivo** final es asegurar que entendemos y compartimos las necesidades y metas de nuestros clientes, intentando prestar servicios que cumplan sus expectativas trabajando en la mejora continua. Manifiesta expresamente su compromiso de potenciar la **Seguridad, Ciberseguridad y Privacidad,** de la Información del servicio prestado con su GRC de ENS, y se compromete a satisfacer las necesidades y expectativas de las partes interesadas, a mantener alta nuestra competitividad en *El Sistema de Información que da soporte a la prestación de los siguientes servicios: Servicio de Mantenimiento, Soporte, Operación y Administración de infraestructura y aplicaciones informáticas. Proyectos de transformación digital de infraestructuras y aplicaciones informáticas y Servicio de Diseño, Arquitectura y Desarrollo de soluciones software*

Esta política de seguridad de la información establece el marco normativo bajo el cual Esvora garantiza la seguridad, confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información tratada en sus sistemas. Se basa en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS), y se complementa con la normativa interna y las guías de buenas prácticas del CCN-CERT.

Esta política aplica a todos los empleados, colaboradores y terceros con acceso a los sistemas de información de Esvora y cubre la totalidad de los activos tecnológicos y procesos críticos de la organización.

MISIÓN y OBJETIVOS*:*

- Fomentar la mejora continua de los servicios al cliente.
- Continuar el posicionamiento de **Esvora** como referente en el sector.
- Implantar, mantener y comprobar nuestros mecanismos de continuidad de la actividad para garantizar que la información y los servicios vitales estén a disposición de nuestros clientes cuando sea necesario.
- Tener una prestación del servicio basada en nuestro compromiso con la mejora continua de nuestros sistemas, con **la seguridad y ciberseguridad y privacidad de la información** como pilar central y por defecto.
- Implantar una cultura de seguridad de la información mediante la formación y la sensibilización.
- Garantizar que nuestros sistemas y redes de información se mantienen y protegen eficazmente frente a amenazas internas y externas y con las garantías legales aplicables. (Consultar Anexo de Requisitos Legales Aplicables)

Nuestra **misión** y objetivos lo conseguiremos a través de:

- Un sistema de **objetivos**, métricas e indicadores de mejora continua, seguimiento, medición de nuestros procesos internos, así como de la satisfacción de nuestros clientes. Estableciendo y supervisando el cumplimiento de los requisitos legales y contractuales para asegurar un servicio eficaz y seguro.
- Formando y concienciando continuamente a nuestro equipo para tener el mayor grado de profesionalidad y especialización posible, además teniendo nuestras infraestructuras en un estado adecuado y en concordancia con los requerimientos legales y de nuestros clientes.
- Con un procedimiento seguro de gestión de adquisición de productos.
- Cumpliendo las exigencias de la legislación vigente y el cumplimiento de nuestros procedimientos de seguridad.
- Introduciendo los procesos de mejora continua que permitan un avance permanente en nuestra gestión de Seguridad de la Información.
- Gestionando y elaborando planes para la gestión y tratamiento de los riesgos con una metodología de análisis y gestión de riesgos utilizada, basada en estándares.
- Gestionando las comunicaciones internas y externas e información almacenada y en tránsito.
- Gestionando y monitorizando la actividad con la gestión de logs.
- Con especial atención a la gestión de incidentes de seguridad
- Asegurando la continuidad y disponibilidad del negocio y de los servicios.
- Esvora ha clasificado sus sistemas de información conforme a lo establecido en el Anexo I del ENS, determinando que estos requieren la aplicación de las medidas de seguridad

correspondientes a un **Nivel ALTO** en las dimensiones de Confidencialidad, Integridad, Disponibilidad, Autenticidad y Trazabilidad
Para ello, se han implementado y documentado las medidas de seguridad descritas en el Anexo II del ENS, garantizando su aplicación efectiva y su supervisión continua mediante auditorías internas y externas.

Así mismo, estos principios se deberán contemplar en las siguientes áreas de seguridad:

- **Física**: Comprendiendo la seguridad de las dependencias, instalaciones, sistemas hardware, soportes y cualquier activo de naturaleza física que trate o pueda tratar información, así como los accesos físicos.
- **Lógica**: Incluyendo los aspectos de protección de aplicaciones, redes, comunicación electrónica, sistemas informáticos y con los accesos lógicos.
- **Político-corporativa:** Formada por los aspectos de seguridad relativos a la propia organización, a las normas internas, regulaciones y normativa legal.

El objetivo último de la seguridad de la información es asegurar que una organización pueda cumplir sus **objetivos** utilizando sistemas de información. En las decisiones en materia de seguridad deberán tenerse en cuenta los siguientes 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 de seguridad y contratación de servicios de seguridad.
- Mínimo privilegio.
- Integridad y actualización del sistema.
- Protección de la información almacenada y en tránsito.
- Prevención ante otros sistemas de información interconectados.
- Registro de la actividad y detección de código dañino.
- Incidentes de seguridad.
- Continuidad de la actividad.
- Mejora continua del proceso de seguridad.

**ROLES O FUNCIONES DE SEGURIDAD**

Roles o funciones de seguridad:

Responsable de la Información: determinará los requisitos (de seguridad) de la información tratada, según los parámetros del Anexo I del ENS.

- 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).

Responsable del sistema: Desarrolla, opera, mantiene y define la topología del sistema

- Tiene las siguientes funciones:

    - Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.
    - Definir la topología y la gestión del sistema de información, estableciendo los criterios de uso y los servicios disponibles en el mismo.
    - Cerciorarse de que las medidas de seguridad se integren adecuadamente en el marco general de seguridad.

Responsable de Seguridad de la Información: Determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

- Las dos funciones esenciales del Responsable de la Seguridad son:

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo con lo establecido en la Política de Seguridad de la Información de la organización.
- Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.

Responsable del Servicio: Determina los requisitos (de seguridad) de los servicios prestados, según los parámetros del Anexo I del ENS.

- Tiene la potestad de establecer los requisitos del servicio en materia de seguridad. La determinación de los niveles en cada dimensión de seguridad se realiza dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad estando los criterios de valoración respaldados por la Política de Seguridad.

El Comité de Seguridad de Esvora con la finalidad de regular y procedimentar las medidas y políticas de seguridad y privacidad de la información, así como de las normativas orientadas a la adaptación de los sistemas de información a la normativa vigente de protección de datos de carácter personal., tiene entre otras funciones:

- Aprobar el inicio de la implantación del SGSI.
- Revisión y aprobación de la Política de Seguridad.
- Aprobación de la Documentación del Sistema de Seguridad y Privacidad de la Información, así como de nuevas ediciones o modificaciones.
- Seguimiento de la implantación y funcionamiento del Sistema de Seguridad de la Información.
- Análisis de reclamaciones planteadas por los clientes
- Evaluar de forma periódica el grado de exposición a riesgos que afecten a los sistemas de información y tratamientos de datos personales de Esvora
- Resolución de conflictos en materia de seguridad de la información, especialmente aquellos derivados de la asignación de responsabilidades, la interpretación de requisitos de seguridad, la priorización de medidas o la gestión de riesgos. A tal efecto:
    - Analizará los conflictos que puedan surgir entre responsables de la información, del servicio, del sistema y de seguridad.
    - Adoptará decisiones basadas en el análisis de riesgos, el cumplimiento normativo y los objetivos de negocio.
    - Garantizará que las decisiones adoptadas mantengan el adecuado equilibrio entre seguridad, operatividad y cumplimiento legal.
    - Documentará las decisiones adoptadas, asegurando su trazabilidad.

Componen el CSI:

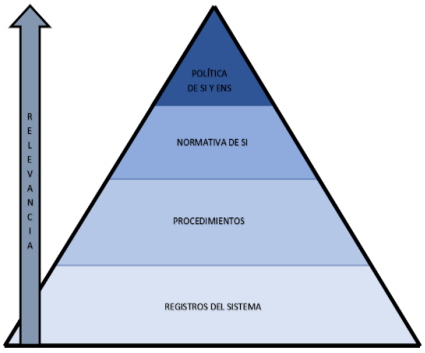
- Responsable de la Información
- Responsable del Servicio
- Responsable de Seguridad de la información
- Responsable del Sistema

Considerando estas pautas, esta dirección reitera su más firme compromiso aunando esfuerzos para el logro de estos objetivos, por lo que esta política es entendida, implantada y mantenida al día en todos los niveles de la organización.

Se entenderá que el rol se renueva automáticamente si no se sustituye o causa baja expresamente

ESTRUCTURA Y CLASIFICACIÓN DE LA INFORMACIÓN:

La documentación del sistema sigue la siguiente estructura:




La clasificación de la información del sistema se clasifica en las siguientes categorías, tal y como se establece en documento Normativa de Seguridad

- Uso Publico
- Uso Interno
- Uso Confidencial

Cada categoría de información está protegida con medidas específicas:

**Uso Público**: No requiere medidas restrictivas, pero se garantiza la autenticidad de la fuente.

**Uso Interno**: Acceso limitado a empleados autorizados. Protección mediante controles de acceso y autenticación.

**Uso Confidencial**: Cifrado obligatorio en tránsito y en reposo, almacenamiento seguro y control de accesos reforzado con autenticación multifactor.

**Legislación aplicable en materia de tratamiento de datos de carácter personal**

En materia de tratamiento de datos de carácter personal se tendrá en cuenta, principalmente, el 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 y la legislación nacional correspondiente.
El marco legal y regulatorio aplicable se encuentran recogido en el documento Registro Identificación y evaluación de requisitos legales.
Los riesgos que se derivan del tratamiento de los datos personales se analizan en el documento Gestión de Riesgos de Privacidad de LOPD
Considerando estas pautas, esta dirección reitera su más firme compromiso aunando esfuerzos para el logro de estos objetivos, por lo que esta política es entendida, implantada y tenida al día en todos los niveles de la organización.

Fdo.

Dirección