

POLÍTICA SEGURIDAD DE LA INFORMACIÓN

La Gerencia de **FORMANOR** define a través de esta Política de Seguridad su compromiso de implantación y mantenimiento de un Sistema de Gestión de Seguridad de la Información, basado en los requisitos de la norma UNE-EN ISO/IEC 27001:2023. La organización establece un SGSI que da soporte a todas las actividades desarrolladas, prestando especial interés al cumplimiento de las políticas y normas de seguridad establecidas, velando por la mejora continua de la seguridad de la información basándose en los siguientes principios:

1. **Integración.** La Seguridad Global es un proceso integrado y alineado con el negocio, en el que participa toda la empresa.
2. **Rentabilidad.** La Seguridad se guía por criterios de negocio, teniendo en cuenta la relación entre gasto e inversión. Sus criterios se fijan de forma centralizada, aprovechando cualquier sinergia existente. Esta gestión permite una reducción global del gasto y un mejor rendimiento del esfuerzo aplicado a la seguridad.
3. **Continuidad.** La seguridad debe de estar presente durante todo su ciclo de trabajo: protección, prevención, detección, respuesta y recuperación.
4. **Adecuación.** Los medios empleados deben adaptarse al entorno del negocio. Entre otros factores, se destacan por su impacto en el negocio y en los niveles de seguridad de la organización la competencia con otras empresas, los desórdenes de índole social, política y económica, el “hacking” amateur o profesional, etc.

Para lograr el cumplimiento de los principios anteriores, es necesario implementar un conjunto de medidas de seguridad, tanto técnicas como organizativas que garanticen la efectividad de los esfuerzos realizados. Todas las medidas adoptadas se establecen a través del Manual de seguridad, los procedimientos y las instrucciones de trabajo definidas.

La responsabilidad última de la seguridad corresponde al Comité de Seguridad que es el responsable directo de gestionar su desarrollo e implantación.

El Comité de Seguridad analizará los riesgos y vulnerabilidades en materia de seguridad que puedan afectar al buen funcionamiento del negocio y propondrá las normas, medios y medidas procedentes para minimizarlas.

Todo el personal de la organización debe asumir la responsabilidad de mantener la seguridad de los activos a su cargo, observando las normas de seguridad que se implanten. Objetivos:

- Conseguir y mantener el nivel de seguridad requerido para garantizar de forma adecuada la continuidad del negocio, incluso en situaciones adversas.
- Incrementar la integración y el apoyo mutuo de los aspectos físicos y lógicos de la seguridad.
- Colaborar en la gestión de las demás disciplinas de seguridad, incluyendo los aspectos laborales y medioambientales, atendiendo a los criterios que potencien la Responsabilidad Social Corporativa.
- Establecer la estructura corporativa de seguridad definida por los órganos de decisión de la organización y crear los canales de comunicación adecuados entre todos los implicados.

POLÍTICA SEGURIDAD DE LA INFORMACIÓN

- Cumplir con la normativa oficial en materia de seguridad y otros requisitos.
- Establecer e implantar Planes de Formación y de Divulgación de Seguridad para mejorar la formación del personal.
- Compromiso expreso de la mejora continua.
- Integrar a los distintos departamentos de la empresa en un sistema de gestión de la seguridad que, bajo criterios comunes, aproveche las sinergias y logre consistencia en los recursos y acciones.
- Todo el personal de la organización conocerá y aplicará la normativa que desarrolle esta Política de Seguridad.

Por último, la Gerencia se compromete a facilitar los medios necesarios y a adoptar las mejoras oportunas en toda la Organización, para fomentar la prevención de los riesgos y daños sobre los activos, mejorando así la eficiencia y eficacia del SGSI.

En Vigo a 15 de Enero de 2024

Firmado: Gerente

