Política de Seguridad de la Información (SGSI)

ISO 27001:2022

NORDLOGWAY, S.L. ha decidido gestionar su **Sistema de Gestión de Seguridad de la Información (SGSI)** conforme a las mejores prácticas internacionales, alineándose con la **ISO/IEC 27001** y la **Directiva (UE) 2022/2555 (NIS2)**.

OBJETIVO DE LA POLÍTICA DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

La Política persigue un doble propósito:

- **Marco de referencia**: establecer las bases que permitan proteger las propiedades de seguridad de los activos que soportan los procesos de NORDLOGWAY. Este marco se fundamenta en los resultados del análisis de riesgos, en los requisitos estratégicos del negocio alineados con la seguridad y en las obligaciones legales y contractuales. En coherencia con lo anterior, la Política fija los principios esenciales que se desarrollan en normas, procedimientos, instrucciones técnicas, registros y demás documentos que concretan el uso adecuado de la información, los sistemas y los activos que los soportan.

- **Medidas de seguridad**: definir las medidas organizativas, físicas y lógicas apropiadas para preservar la seguridad de dichos activos, partiendo de que la seguridad es un **proceso integral y transversal** (que abarca componentes técnicos, humanos, materiales y organizativos de los sistemas de información y comunicaciones) y que debe concebirse como **inversión** para prevenir impactos negativos en el negocio, no como un mero coste.

ÁMBITO DE APLICACIÓN

Esta Política es aplicable a los Sistemas de Información que sustentan todos los procesos de NORDLOGWAY en el desarrollo de sus actividades. Cualquier normativa, procedimiento o documento interno que trate aspectos específicos de seguridad de los Sistemas de Información deberá respetar y cumplir lo establecido en esta Política.

La Política aplica a **todas las personas** que intervienen en las actividades y procesos de negocio dentro del alcance del SGSI: empleados, socios, colaboradores y terceros.

PRINCIPIOS FUNDAMENTALES Y OBJETIVOS

1. Cumplimiento normativo: los sistemas de información se ajustarán a la normativa legal, regulatoria y sectorial aplicable a la seguridad de la información, con especial atención a la protección de datos personales y a la seguridad de sistemas, datos, comunicaciones y servicios electrónicos.

2. Gestión del riesgo: los riesgos deberán reducirse a niveles aceptables, buscando el equilibrio entre controles de seguridad y naturaleza de la información. Los objetivos de seguridad se establecerán, revisarán periódicamente y serán coherentes con los requisitos de seguridad de la información.

3. Concienciación y formación: se implantarán programas de capacitación, sensibilización y campañas de concienciación en materia de seguridad para todos los usuarios con acceso a la información.

4. Confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad:

- **Confidencialidad**: solo las personas autorizadas podrán acceder a la información.
- **Integridad**: la información deberá mantenerse exacta y completa, garantizando la precisión de su contenido y de los procesos asociados.
- **Disponibilidad**: la información y los servicios deberán estar disponibles cuando se requieran, asegurando la continuidad del negocio mediante planes de contingencia.
- **Autenticidad**: se garantizará la identidad de las entidades (personas o procesos) que traten la información.
- **Trazabilidad**: las actuaciones sobre la información deberán poder atribuirse de forma indiscutible a la entidad que las realizó.

5. Proporcionalidad: la implantación de controles de seguridad para mitigar riesgos se realizará guardando equilibrio entre las medidas aplicadas, la naturaleza de la información y el riesgo existente.

6. Responsabilidad: todos los miembros de NORDLOGWAY deberán actuar responsablemente en materia de seguridad de la información y cumplir las normas y controles establecidos.

7. Mejora continua: la Dirección asume la responsabilidad de promover la mejora continua del Sistema de Gestión de la Seguridad de la Información, asegurando que los controles implantados se revisen y refuercen regularmente para anticiparse a la evolución del riesgo y del entorno tecnológico.

Esta Política constituye el marco de referencia para el establecimiento de los objetivos de seguridad.

CONTINUIDAD DE NEGOCIO

NORDLOGWAY dispone de un Plan de Continuidad de Negocio para garantizar la disponibilidad de los sistemas y servicios críticos. En particular, se han definido:

- **Plan de Continuidad de Negocio.**
- **Análisis de Impacto en el Negocio (BIA).**
- **Plan de Recuperación ante Desastres (DRP).**

El Plan de Continuidad está diseñado para sostener la operación de las actividades clave de soporte de NORDLOGWAY, disminuir el daño y el impacto de incidentes imprevistos sobre los servicios y acelerar la recuperación de la actividad.

TERCERAS PARTES

Cualquier tercero que acceda a información de NORDLOGWAY, en el marco de una prestación de servicios, deberá conocer esta Política y su normativa asociada, y comprometerse a cumplir las obligaciones derivadas de la misma, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se exigirá que el personal de dichos terceros esté adecuadamente concienciado en seguridad, al menos con el mismo nivel requerido en esta Política.

CONTACTO

Para cualquier información adicional sobre esta Política o para trasladar sugerencias, puede escribir a:
info@nordlogway.com

Víctor Gastón Puyo
Director General de Nordlogway
10 de julio de 2025