POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

NORDLOGWAY

OBJETIVO

Proteger la información, los sistemas y los activos que dan soporte a los procesos de NORDLOGWAY, mediante un SGSI alineado con ISO/IEC 27001:2022 y la Directiva (UE) 2022/2555 (NIS2).

ÁMBITO Y COMPROMISO

Aplicable a todos los sistemas de información y a todas las personas que participan en los procesos: empleados, socios, colaboradores y terceros. La seguridad se gestiona como un proceso integral, transversal y orientado a la mejora continua.

Víctor Gastón Puyo
Director General de Nordlogway

28/09/2026 POL-SGSI-01 rev 02

NORD LOGWAY
OPERADOR LOGÍSTICO

01
CUMPLIMIENTO NORMATIVO
Cumplimos la normativa legal, reguladora y sectorial aplicable, con especial atención a la protección de datos y a la seguridad de los sistemas, datos, comunicaciones y servicios.

02
GESTIÓN DEL RIESGO
Identificamos, analizamos y reducimos los riesgos a niveles aceptables, manteniendo el equilibrio entre los controles, la naturaleza de la información y el riesgo existente.

03
OBJETIVOS DE SEGURIDAD
Establecemos y revisamos periódicamente objetivos coherentes con los requisitos de seguridad de la información y con las necesidades estratégicas del negocio.

04
SENSIBILIZACIÓN Y FORMACIÓN
Impulsamos programas de capacitación y concienciación para todas las personas usuarias con acceso a la información.

05
CONFIDENCIALIDAD
Garantizamos que solo las personas autorizadas puedan acceder a la información.

06
INTEGRIDAD Y AUTENTICIDAD
Mantenemos la información exacta y completa, y garantizamos la identidad de las personas o procesos que la tratan.

07
DISPONIBILIDAD
Aseguramos que la información y los servicios estén disponibles cuando se necesiten, con medidas orientadas a la continuidad del negocio.

08
TRAZABILIDAD
Garantizamos que las actuaciones sobre la información puedan atribuirse de manera indiscutible a quien las ha realizado.

09
RESPONSABILIDAD Y PROPORCIONALIDAD
Todas las personas deben cumplir las normas y controles, aplicando medidas proporcionadas a la información y a los riesgos.

10
CONTINUIDAD DE NEGOCIO
Disponemos de Plan de Continuidad, Análisis de Impacto en el Negocio (BIA) y Plan de Recuperación ante Desastres (DRP).

11
TERCERAS PARTES
Los terceros con acceso a información deben conocer y cumplir esta política, gestionar incidencias y mantener un nivel adecuado de concienciación.

12
MEJORA CONTINUA
Revisamos y reforzamos regularmente el SGSI y sus controles para anticiparnos a la evolución de los riesgos y del entorno tecnológico.