



POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Fecha: 10/2025

Versión: 0.1

Este documento ha sido generado por Nolter para uso exclusivo de Nolter y su contenido es confidencial. Este documento no puede ser difundido a terceros, ni utilizado para otros propósitos que los que han originado su entrega, sin el previo permiso escrito de Nolter. En el caso de ser entregado en virtud de un contrato, su utilización y difusión estarán limitadas a lo expresamente autorizado en dicho contrato. Nolter no podrá ser considerada responsable de eventuales errores u omisiones en la edición del documento

Control de Versiones

| Versión | Fecha | Autor | Estado | Comentarios |
|---------|---------|----------------------|-----------------|-------------|
| 0.1 | 11/2025 | Pedro José Agra Lago | Versión Inicial | |
| | | | | |
| | | | | |

Resumen de estados:

- Versión inicial: versión 0.1
- Versión Intermedia: versiones que no son la inicial, ni las aprobadas (0.2, 1.1, 2.1,...)
- Pendiente Aprobación: versión intermedia preparada para ser aprobada
- Aprobado: versiones “.0” identificadas con números enteros (p.e. 1.0, 2.0,...)

| | |
|---------------------------|----------------------|
| Responsable del documento | Pedro José Agra Lago |
|---------------------------|----------------------|



Índice

| | |
|--|---|
| 1. INTRODUCCIÓN..... | 4 |
| 2. ALCANCE | 4 |
| 3. MISIÓN | 4 |
| 4. PRINCIPIOS RECTORES DE LA POLÍTICA..... | 5 |
| 5. MARCO NORMATIVO | 6 |
| 6. ORGANIZACIÓN DE LA SEGURIDAD | 6 |
| 7. PROCEDIMIENTO DE DESIGNACIÓN | 7 |
| 8. RESOLUCIÓN DE CONFLICTOS..... | 7 |
| 9. TRATAMIENTO DE DATOS PERSONALES | 7 |
| 10. DESARROLLO DE LA POLÍTICA DE SEGURIDAD..... | 7 |
| 11. OBLIGACIONES DEL PERSONAL | 8 |
| 12. TERCERAS PARTES – PROVEEDORES – SERVICIOS EN LA NUBE | 8 |
| 13. GESTIÓN DE INCIDENTES DE SEGURIDAD | 8 |
| 14. APROBACIÓN Y ENTRADA EN VIGOR | 8 |



1. INTRODUCCIÓN

La presente Política de Seguridad de la Información (PSI) establece el marco global para gestionar la seguridad de la información en Nolter, garantizando una protección adecuada de la información tratada y de los servicios prestados por la entidad. Su objetivo es asegurar la continuidad de las operaciones, el cumplimiento de los objetivos de negocio y el alineamiento con el Esquema Nacional de Seguridad (ENS).

La PSI define los principios, objetivos y directrices que guían a la organización en la gestión de la seguridad de la información, conforme a las buenas prácticas nacionales y a la realidad de Nolter. Los datos específicos que sea necesario completar (p. ej., fechas o nombres) se dejan en blanco para su cumplimentación.

2. ALCANCE

Esta Política es de aplicación general en Nolter. En particular, alcanza:

- Sistemas de información y comunicaciones: todos los sistemas, infraestructuras tecnológicas, aplicaciones, bases de datos y comunicaciones electrónicas gestionados por Nolter, con independencia de su ubicación o soporte.
- Información y datos: toda la información tratada, almacenada o transmitida en la organización, incluidos datos personales, datos de clientes, información corporativa y demás activos informacionales relevantes.
- Personal: todo el personal de Nolter (empleados, dirección y colaboradores internos o externos) que acceda o maneje información de la entidad, incluyendo personal temporal, becarios y contratistas.
- Proveedores y terceros: cualquier entidad externa que preste servicios a Nolter y que, en ese marco, acceda a información o sistemas de la organización. Estos terceros deberán cumplir las obligaciones de seguridad aplicables.

El alcance cubre personas, procesos y tecnologías relacionadas con la información de Nolter. Toda nueva incorporación (sistema, empleado o proveedor) queda sujeta a esta Política desde el inicio de su relación con la organización. Esta Política se complementa con políticas y procedimientos específicos publicados en el repositorio documental interno.

3. MISIÓN

La misión de Nolter es proporcionar servicios profesionales de ingeniería y medio ambiente con la máxima calidad, eficiencia y continuidad. En coherencia con ello, la misión en materia de seguridad de la información consiste en garantizar que los activos de información y los sistemas tecnológicos que soportan dichos servicios, incluyendo procesos, aplicaciones, datos, infraestructuras, dispositivos y servicios de terceros o en la nube, estén adecuadamente protegidos. Esta protección se materializa asegurando la disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad de la información a lo largo de todo su ciclo de vida, desde la creación y el tratamiento hasta el archivo y la eliminación segura.

Para alcanzar esa misión, Nolter integra la seguridad en la estrategia de negocio y en el funcionamiento diario de la organización, adoptando un enfoque basado en riesgos y la mejora continua. La seguridad se aplicará por diseño y por defecto en los servicios y proyectos, procurando que las medidas sean proporcionales al impacto potencial y que no obstaculicen la operativa ni la calidad del servicio al cliente.

Los objetivos de seguridad de Nolter se concretan en: mantener la prestación continua de los servicios críticos, reduciendo la superficie de exposición y estableciendo capacidades de resiliencia; proteger la calidad y exactitud de la información y de los registros que soportan las decisiones de negocio; preservar la privacidad de los datos personales y el secreto profesional de la información confidencial; cumplir las obligaciones legales, reglamentarias y contractuales (incluido el ENS y la normativa de protección de datos); fortalecer la resiliencia operativa mediante copias de seguridad, pruebas periódicas de restauración y planes de continuidad; impulsar la concienciación y formación del personal para prevenir errores y fraudes; y asegurar una gestión adecuada de terceros, exigiendo medidas equivalentes a las internas cuando acceden a información o sistemas.

Asimismo, Nolter se compromete a disponer de responsables designados, a realizar análisis de riesgos y categorización de sistemas con la periodicidad adecuada, a documentar políticas y procedimientos que desarrollen esta Política, a gestionar y notificar incidentes conforme a los canales establecidos, y a someter el conjunto del sistema de seguridad a revisiones y auditorías periódicas, informando a la Dirección de los resultados y planes de mejora.

4. PRINCIPIOS RECTORES DE LA POLÍTICA

Nolter adopta los principios básicos del ENS, que inspiran esta Política y se concretan en los siguientes principios y compromisos:

1. Seguridad como proceso integral. La seguridad se aplica de forma transversal a personas, procesos, tecnologías y proveedores, a lo largo de todo el ciclo de vida de la información y de los servicios. Nolter integrará la seguridad en la planificación, el diseño, la adquisición, la operación y la baja de activos, promoviendo la concienciación del personal y la coordinación entre los responsables designados.
2. Gestión de la seguridad basada en riesgos. Las decisiones de seguridad se adoptarán con base en análisis de riesgos periódicos y en la categorización de sistemas. Se priorizarán las medidas en función del impacto y la probabilidad, documentando el tratamiento (reducción, aceptación, transferencia o evitación) y revisándolo cuando cambien los servicios, la tecnología o el contexto.
3. Prevención, detección, respuesta y recuperación. Nolter establecerá medidas preventivas (configuración segura, parcheo, control de accesos, formación), capacidades de detección (monitorización y registro de eventos relevantes), procedimientos de respuesta ante incidentes (contención, erradicación, recuperación, comunicación) y actividades de mejora (lecciones aprendidas), preservando evidencias cuando proceda.
4. Defensa en profundidad (líneas de defensa). La protección se articulará en capas complementarias y redundantes: organizativas, físicas y lógicas. Se aplicarán, entre otras, segregación de funciones, principio de mínimo privilegio, segmentación de redes, autenticación reforzada cuando sea necesario y copias de seguridad verificadas.

5. Vigilancia continua. Se mantendrán mecanismos de supervisión proporcional al riesgo para identificar eventos anómalos, vulnerabilidades y desviaciones de configuración. Los indicadores y umbrales definidos permitirán actuar de forma temprana, y se informará a la Dirección de la evolución del estado de seguridad con una periodicidad definida.
6. Reevaluación periódica. Las medidas se revisarán de manera regular y tras cambios significativos o incidentes relevantes, comprobando su eficacia y adecuación. Se realizarán auditorías y revisiones internas en función de la categoría de los sistemas y del marco ENS, generando planes de acción y seguimiento.
7. Diferenciación de responsabilidades. Las funciones de seguridad se asignarán a roles definidos (Responsable de la Seguridad, del Sistema, del Servicio y de la Información), garantizando, en la medida de lo posible, la independencia funcional y los controles cruzados. Cuando una misma persona asuma varios roles, se adoptarán salvaguardas de revisión y supervisión para evitar conflictos de interés.

Estos principios son de obligado cumplimiento y guían el desarrollo normativo y los procedimientos específicos de seguridad de Nolter.

5. MARCO NORMATIVO

Esta política se alinea con el marco legal y normativo vigente que define el ámbito de actuación de Nolter. En particular, se rige por:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS), que establece los principios y requisitos mínimos de seguridad aplicables y guía la categorización de los sistemas.
- Reglamento (UE) 2016/679 (RGPD) y Ley Orgánica 3/2018 (LOPDGDD), relativos a la protección de datos personales, incluidos sus principios y obligaciones para responsables y encargados del tratamiento.
- Normas ISO/IEC 27001/27002 y familia (p. ej., ISO 27005 para gestión de riesgos, ISO 27035 para gestión de incidentes), en la medida en que complementen los requisitos del ENS.
- Instrucciones Técnicas de Seguridad (ITS) del ENS y guías CCN-STIC (especialmente la serie 800), como referencia para la implantación práctica de medidas y controles.
- Contratos y cláusulas con clientes y proveedores, que establezcan requisitos de seguridad, confidencialidad, continuidad y niveles de servicio (SLA), incluyendo condiciones específicas para servicios en la nube.
- Cualquier otra ley, reglamento o disposición específica que resulte de aplicación a la información o a los sistemas gestionados por Nolter, atendiendo a su actividad y compromisos contractuales.

6. ORGANIZACIÓN DE LA SEGURIDAD

Nolter no constituye un comité de seguridad dada su dimensión. La coordinación y seguimiento en materia de seguridad se realizan directamente entre los responsables designados (Responsable de la Seguridad, del Sistema, del Servicio y de la Información), conforme al ENS, bajo supervisión de la

Dirección. Una misma persona puede asumir varios roles si ello no compromete el correcto desempeño de sus funciones.

Funciones de coordinación (roles designados):

- Alinear las actividades de la organización en materia de seguridad (información, seguridad física vinculada, cumplimiento y continuidad), asegurando coherencia entre políticas, normas y procedimientos.
- Integrar los diferentes modelos de gobernanza aplicables (ENS, RGPD y, cuando proceda, NIS2, CER, IA, etc.).
- Elaborar y proponer la revisión de esta Política y de su desarrollo documental.
- Supervisar la gestión de riesgos a nivel corporativo, promoviendo análisis continuos que orienten las actividades de seguridad.
- Impulsar la mejora continua, la formación y concienciación y el seguimiento del cumplimiento.
- Resolver conflictos o discrepancias que no hayan podido solucionarse a nivel operativo, elevándolos a Dirección cuando proceda.

Los responsables se reunirán al menos una vez al año para revisar el estado de la seguridad y coordinar acciones.

7. PROCEDIMIENTO DE DESIGNACIÓN

Las figuras ENS de Responsable de la Información, del Servicio, del Sistema y de la Seguridad están designadas formalmente en el documento “Acta de Constitución de Roles y Responsabilidades ENS”, donde constan sus nombres y funciones.

8. RESOLUCIÓN DE CONFLICTOS

En caso de conflictos entre responsables o entre áreas, se intentarán resolver en el ámbito operativo. Si persisten, se elevarán al RSI y, en su caso, a Dirección para su decisión.

9. TRATAMIENTO DE DATOS PERSONALES

Nolter se compromete firmemente a la protección de los datos personales tratados y al cumplimiento estricto de la normativa de privacidad vigente.

Todas las actividades de tratamiento de datos personales realizadas por Nolter, se ajustan a los principios y obligaciones establecidos en el Reglamento General de Protección de Datos (RGPD) y en la Ley Orgánica 3/2018 (LOPDGDD). Esto incluye, entre otros, el respeto a los principios de licitud, lealtad y transparencia, minimización de datos, limitación de la finalidad, exactitud, limitación del plazo de conservación, integridad y confidencialidad, así como la atención a los derechos de los interesados (acceso, rectificación, supresión, etc.).

Nolter no está incluida en los supuestos que exigen designar Delegado/a de Protección de Datos (DPD) conforme al art. 37.1 del RGPD y al art. 34 de la LOPDGDD; por tanto, no resulta obligatorio su nombramiento en la actualidad.

Mientras no proceda, el Responsable de la Seguridad de la Información (RSI) actuará como punto de contacto de privacidad, coordinando el cumplimiento del RGPD/LOPDGDD, la atención de derechos y la gestión/notificación de brechas. Si en el futuro Nolter pasara a encajar en dichos supuestos, designará un DPD, publicará su contacto y lo comunicará a la AEPD, actualizando esta Política.

10. DESARROLLO DE LA POLÍTICA DE SEGURIDAD

La presente Política se desarrolla e implementa a través de procedimientos, instrucciones y controles documentados que han sido elaborados teniendo en cuenta los estándares nacionales e internacionales de referencia y forman parte del repositorio documental interno de Nolter.

11. OBLIGACIONES DEL PERSONAL

Todo el personal deberá conocer y cumplir esta Política y sus desarrollos; proteger credenciales y dispositivos; utilizar únicamente medios autorizados; custodiar la información según su clasificación; y comunicar inmediatamente cualquier incidente o sospecha por los canales establecidos.

12. TERCERAS PARTES – PROVEEDORES – SERVICIOS EN LA NUBE

Cuando Nolter preste servicios a otras entidades o maneje información de otras, se les hará partícipes de esta Política, sin perjuicio de respetar las obligaciones de la normativa de protección de datos si actúa como encargado del tratamiento en la prestación de los citados servicios, y se establecerán canales para reporte y coordinación de las actuaciones para la reacción ante incidentes de seguridad.

13. GESTIÓN DE INCIDENTES DE SEGURIDAD

Nolter dispone de un procedimiento para la gestión ágil de los eventos e incidentes de seguridad que supongan una amenaza para la información y los servicios. Este procedimiento se integra con todos los procesos de la compañía para coordinar la respuesta desde los diferentes enfoques y comunicar a los diferentes organismos de control sin dilaciones indebidas y, cuando sea preciso, a las Fuerzas y Cuerpos de Seguridad el Estado o los juzgados.

14. APROBACIÓN Y ENTRADA EN VIGOR

Esta Política se aprueba por la Dirección de Nolter y entra en vigor en la fecha indicada. Será aplicable a toda la organización y a terceros con acceso a su información.

La revisión de esta Política se realizará, como mínimo, cada dos años o cuando se produzcan cambios relevantes. La Política y sus modificaciones se informarán adecuadamente a los interesados por los mismos canales usados para su difusión.

Firmado digitalmente
por 09277155J EMILIO
VILLAR (R: B26321745)

D. Emilio Villar González
Dirección Nolter

Logroño, __ de _____ de 2025