POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

POL-01

Nivel de confidencialidad | Público

Historial de modificaciones

Fecha	Versión	Modificado por	Descripción de la modificación
16/03/2026	1	CISO - Notin	Versión inicial

1. Introducción

Notin depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos de negocio. El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza ante incidentes. Los sistemas deben protegerse frente a amenazas de rápida evolución que puedan incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información.

La estrategia de seguridad se articula en torno a tres ejes:

Prevención

Los departamentos implementarán las medidas mínimas del ENS junto con controles adicionales derivados del análisis de riesgos. Todos los sistemas deben ser autorizados antes de entrar en operación y sometidos a evaluaciones periódicas, incluyendo cambios de configuración.

Detección

Los servicios monitorizarán su operación de forma continua para detectar anomalías (Art. 9 ENS). Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y ante desviaciones significativas de los parámetros normales (Art. 8 ENS).

Respuesta

Los departamentos deberán:

- Establecer mecanismos eficaces de respuesta a incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones sobre incidentes.
- Establecer protocolos de intercambio de información con los CERT (comunicación bidireccional).

2. Alcance

Esta política se aplica a todos los sistemas TIC de Notin y a todos sus miembros, sin excepción alguna.

3. Misión y Principios del SGSI

La Dirección de Notin asume el deber de garantizar la seguridad de la información como elemento esencial para el correcto desempeño de sus servicios. Los principios rectores del Sistema de Gestión de Seguridad de la Información (SGSI) son:

- Implementar la cultura de seguridad en toda la organización.
- Preservar la confidencialidad, integridad, disponibilidad y resiliencia de la información.
- Proteger los activos de información frente a amenazas internas, externas, deliberadas o accidentales.
- Establecer un plan de seguridad que integre la prevención y minimización de riesgos.
- Proveer los recursos necesarios para la gestión de riesgos identificados.
- Asumir la responsabilidad en concienciación y formación en seguridad de la información.
- Extender el compromiso de seguridad a personal trabajador y proveedores.
- Mejorar continuamente mediante el seguimiento periódico de objetivos de seguridad.

En materia de datos personales, los datos se tratarán conforme a los principios del RGPD: licitud, lealtad y transparencia; limitación de la finalidad; minimización de datos; exactitud; limitación del plazo de conservación; e integridad y confidencialidad.

Esta Política será revisada a intervalos planificados o ante cambios significativos, a fin de asegurar su idoneidad, adecuación y eficacia.

4. Marco Normativo

La gerencia de Notin se asegura de que la documentación de origen externo de interés para la empresa sea conocida, actualizada y disponible. Los documentos de referencia son:

- Esquema Nacional de Seguridad (ENS — RD 311/2022)
- Guía CCN-STIC-801
- Guías CCN, Abstracts, CoCENS y normativa aplicable a Notin

5. Organización de la Seguridad

Se ha constituido un Comité de Seguridad formado por: Dirección general, responsable de seguridad, responsable de los sistemas, responsable de protección de datos, responsable de la información y responsable del servicio.

Sus funciones principales son:

- Obtener una visión del estado de la seguridad de la información.
- Revisar la Política, Normativa y procedimientos al menos anualmente.
- Aprobar los requisitos de formación y priorizar actuaciones.
- Promover auditorías del SGSI y técnicas.
- Garantizar que la Seguridad de la Información está presente en todos los proyectos.

6. Roles: Funciones y Responsabilidades

Rol	Responsabilidades principales
Dirección ejecutiva	Aprueba políticas y revisiones por dirección del SGSI. Valida conclusiones de auditorías. Define objetivos y mediciones.

Responsable de seguridad	Promueve y supervisa el SGSI conforme al ENS. Establece medidas de seguridad, coordina análisis de riesgos, promueve auditorías y formación.
Responsable del sistema	Desarrolla, opera y mantiene los sistemas TIC. Integra medidas de seguridad en el ciclo de vida. Monitoriza estado de seguridad e informa incidentes.
Responsable de protección de datos	Asesora sobre obligaciones RGPD/LOPDGDD. Supervisa cumplimiento normativo. Actúa como punto de contacto con la AEPD. Supervisa las EIPD.
Responsable del servicio	Define requisitos de seguridad del servicio (interoperabilidad, accesibilidad, disponibilidad). Determina niveles de seguridad.
Responsable de la información	Vela por el uso correcto de la información. Define requisitos y niveles de seguridad de la información tratada.
Usuarios y empleados	Conocen y cumplen esta Política y la normativa de seguridad. Protegen la información de la empresa.

Cualquier conflicto entre responsables que no se resuelva de común acuerdo será elevado a la Dirección de Notin, cuya decisión será vinculante y quedará documentada.

7. Gestión de Riesgos

Todos los sistemas sujetos a esta Política realizarán un análisis de riesgos evaluando las amenazas y riesgos a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos una vez al año.
- Cuando cambie la información manejada o los servicios prestados.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

El Comité de Seguridad TIC establecerá una valoración de referencia para los distintos tipos de información y servicios, y dinamizará la disponibilidad de recursos para atender las necesidades de seguridad.

8. Obligaciones del Personal

Todos los miembros de Notin tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad. Además:

- Asistirán al menos a una sesión anual de concienciación en seguridad TIC.
- Existirá un programa de concienciación continua, especialmente para nuevas incorporaciones.
- Las personas con responsabilidad en la operación de sistemas recibirán formación específica, obligatoria antes de asumir dicha responsabilidad.

9. Terceras Partes

Cuando Notin preste servicios a otros organismos o maneje su información, les hará partícipes de esta Política y establecerá canales de coordinación entre los respectivos Comités de Seguridad.

Cuando Notin utilice servicios de terceros o les ceda información, dichos terceros quedarán sujetos a la Política y Normativa de Seguridad aplicable y deberán garantizar que su personal esté adecuadamente concienciado. Ante incumplimientos, el responsable de Seguridad emitirá un informe de riesgos que requerirá aprobación por los responsables afectados.