

# Política de Seguridad de la Información (SGSI)

NOVANOTIO, que presta servicios de consultoría para grandes integradores tecnológicos, considera que la información y los sistemas asociados son activos críticos que deben ser protegidos para asegurar el correcto funcionamiento de la empresa.

La Política de Seguridad de NOVANOTIO refleja los conceptos, principios, responsabilidades y objetivos en materia de seguridad de la información, cuyos resultados permiten a nuestra empresa alcanzar su propósito de ofrecer servicios de comunicación de todo tipo a nuestros clientes.

Mediante la elaboración, comunicación y mantenimiento de esta política, la Dirección de NOVANOTIO muestra su compromiso de proteger la **confidencialidad** de la información con la que opera en la prestación de sus servicios, garantizar su **integridad** en todos los procesos de tratamiento que lleve a cabo, así como la **disponibilidad** de los sistemas de información implicados en estos tratamientos.

Para ello se compromete a implementar, mantener, supervisar y mejorar de forma continua un **Sistema de Gestión de la Seguridad de la Información (SGSI)**, sostenido por una serie de principios que constituyen a su vez la base de sus objetivos estratégicos:

- La seguridad en la Gestión de los Recursos Humanos antes, durante y al finalizar el empleo.
- La gestión adecuada de los activos que implique la clasificación de la información y la manipulación de los soportes.
- El establecimiento de un robusto control de acceso lógico a sus sistemas y aplicaciones, gestionando los permisos y los privilegios de los usuarios.
- La protección de las instalaciones y del entorno físico, mediante el diseño de áreas de trabajo seguras y la seguridad de los equipos.
- La garantía de la seguridad en las operaciones mediante la protección contra el software malicioso, la realización de copias de seguridad, el establecimiento de registros y su supervisión, el control del software en explotación y la gestión de las vulnerabilidades técnicas.
- La seguridad de las comunicaciones, protegiendo las redes y el intercambio de Información.
- El aseguramiento de la seguridad en la adquisición y mantenimiento de los sistemas de información, limitando y gestionando el cambio.
- La realización de un desarrollo seguro de software, separando los entornos de desarrollo y producción, y realizando las pruebas funcionales de aceptación adecuadas.
- El control de las relaciones con los proveedores, exigiendo de forma contractual el cumplimiento de las medidas de seguridad pertinentes y unos niveles aceptables en la prestación de sus servicios.
- La eficacia en la gestión de los incidentes de seguridad, estableciendo los canales adecuados para su notificación, respuesta y aprendizaje oportuno.
- La realización de un plan de continuidad de negocio que proteja la disponibilidad de los servicios durante una crisis o desastre.
- La Identificación y cumplimiento de la normativa aplicable poniendo especial interés en la propiedad intelectual y en la protección de los datos de carácter personal.
- La revisión periódica de los presentes requerimientos de la seguridad de la información para garantizar el cumplimiento y eficacia de éstos.

Con este fin, la Dirección proporciona los recursos necesarios y pertinentes y mantiene esta política a disposición de sus grupos de interés.