POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE NETWORK SOLUTIONS CONTROL, S.L.

La actividad de **NETWORK SOLUTIONS CONTROL, S.L. (NSC)** es consciente de la relevancia de la seguridad de la información. Por ello ha implantado un Sistema de Seguridad de la Información, basado en ISO 27001 y en el ENS (Esquema Nacional de Seguridad), cuyo alcance es:

"El servicio de control presencial de NSC y a todos los sistemas TIC y miembros de NSC relacionados con el mismo".

El Sistema de Seguridad de la Información tiene una categoría media del ENS.

En **NSC la información es un activo fundamental** para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un **compromiso expreso de protección** de sus propiedades más significativas como parte de una estratégica orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad.

La Política de Seguridad se define como aquel conjunto de directrices plasmadas en documento escrito, que rigen la forma en que la organización **gestiona y protege la información** y los servicios que considera críticos.

La Dirección quiere dar a conocer, a través de este documento, a sus **partes interesadas**, su convencimiento de que la Seguridad de la Información es un factor clave para el correcto desarrollo de la organización. Para ello, ha definido un conjunto de principios, procedimientos y medidas (preventivos, reactivos y de control) para proteger la información que gestiona electrónicamente y sus servicios esenciales, con el **objeto de garantizar la seguridad y la continuidad del negocio**.

La Dirección es responsable de organizar las funciones y responsabilidades, la Política de Seguridad de la Información, y de facilitar los recursos adecuados para **alcanzar los objetivos** propuestos.

El objetivo principal de esta Política de Seguridad de la Información es **asegurar la confidencialidad, integridad, trazabilidad, autenticidad y disponibilidad de los datos**. Será revisada anualmente y siempre que se produzcan incidencias graves de seguridad.

La Dirección concretará los objetivos de seguridad de **NSC** anualmente en la Revisión del Sistema. Al fijar dichos objetivos, se establecerán los responsables, los medios y acciones necesarias a realizar para poder alcanzar los mismos.

La Dirección está comprometida con la **Mejora Continua** del Sistema de Gestión de la Seguridad de la Información.

Esta Política muestra el compromiso de la Dirección y se definen los siguientes objetivos principales:

- Compromiso con el cumplimiento de los requisitos aplicables a la Seguridad de la Información.
- Proteger los servicios e información contra pérdidas de disponibilidad y contra accesos no autorizados.
- Evitar usos maliciosos de la red y accesos no autorizados a los sistemas.
- Preservar confidencialidad e integridad de la información.
- Formar a las personas con responsabilidad en el uso o administración de sistemas TIC para garantizar una operación segura de los mismos y concienciar a toda la organización en la importancia del cumplimiento de esta política.
- Establecer procedimientos de salvaguarda idóneos, incluida la notificación de incidencias de seguridad en el desarrollo de servicios para y por terceros.

NSC está vinculado al siguiente **Marco Normativo** de cumplimiento obligado.

- Real Decreto-ley 8/2019, de 8 de marzo, de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.
- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS): Real Decreto que tiene por objeto determinar la política de seguridad en la utilización de medios electrónicos en su ámbito de

aplicación, y está constituido por los principios básicos y requisitos mínimos que permiten una protección adecuada de la información.

- ITS de Conformidad con el Esquema Nacional de Seguridad y del Informe del Estado de la Seguridad (BOE del 2 de noviembre de 2016): Instrucción técnica que establece los procedimientos para dar publicidad a la conformidad con el Esquema Nacional de Seguridad, así como los requisitos exigibles a las entidades certificadoras.
- Instrucción Técnica de Seguridad de Auditoría (BOE del 3 de abril de 2018): Instrucción técnica que establece las condiciones para la realización de las auditorías, ordinarias o extraordinarias, previstas en el artículo 34 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Reglamento (UE) 2016/679 General de Protección de Datos (RGPD): Reglamento que armoniza la protección de los derechos y las libertades fundamentales de las personas físicas en relación con las actividades de tratamiento de datos de carácter personal, y garantiza la libre circulación de estos datos entre los Estados miembros.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD): Ley que adapta el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, completa sus disposiciones, y garantiza los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución.
- Orden SND/414/2020, de 16 de mayo, para la flexibilización de determinadas restricciones de ámbito nacional establecidas tras la declaración del estado de alarma en aplicación de la fase 2 del Plan para la transición hacia una nueva normalidad.

Para dar respuesta al compromiso legal, **NSC** ha redactado un listado de artículos de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, de obligado cumplimiento.

- **Descubrimiento y revelación de Secretos**. Artículos 197.1, 197.2 y 197.7
- **Acceso ilícito a sistemas informáticos**. Artículos 197 bis1, 197 bis2 y 197 ter
- **Daños informáticos. Artículos**. 264, 264 bis y 264 ter
- **Estafa informática**. Artículos 248, 248.2, 249, 250 y 251
- **Ciberdelitos Sexuales**. Artículos: 181, 182, 183, 183 ter1, 183 ter2, 184, 185, 186, 187, 188, 189 y 189 bis
- **Delitos contra la propiedad intelectual**. Artículos 270.1, 270.2, 270.5 (apartados C y D) y 270.6
- **Amenazas y coacciones**. Artículos 169, 170, 171, 171.2, 172, 172 bis y 172 ter
- **Delitos contra el honor**. Artículos: 205, 208 y 211

Es responsabilidad de toda la organización de **NSC**, el obligado cumplimiento de lo establecido en el SGSI, así como las políticas internas de la organización.

La seguridad es compromiso de TODOS, debe ser conocida por TODOS.

Dirección General

Madrid, a 21 de febrero de 2023