POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LOGIC SH COMPUTING, S.L.

Preparado por:	Revisado por:	Aprobado por:
Responsable de Seguridad	Comité de Seguridad	

Control de modificaciones

Rev nº	Fecha	Descripción
1	02-08-2021	Edición inicial
2	24-01-2022	Se especifica la categoría del ENS
3	21-02-2023	Se añaden artículos del Código Penal
4	24-02-2025	Se actualiza Real Decreto ENS de 3/2010 a 311/2022
5	02-12-2025	Inclusión del apartado “Gestión del Riesgo y Declaración de Aplicabilidad (SoA)” y actualización del marco legal

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

La actividad de **LOGIC SH COMPUTING, S.L. (LSH)** 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 LSH y a todos los sistemas TIC y miembros de LSH relacionados con el mismo”.

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

En **LSH 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.

Este documento es CONFIDENCIAL y no se puede reproducir ni total ni parcialmente sin el consentimiento explícito y por escrito de NSC

La Dirección concretará los objetivos de seguridad de **LSH** 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.

Gestión del Riesgo y Declaración de Aplicabilidad (SoA)

La organización dispone de un análisis de riesgos formalizado conforme a metodologías reconocidas por el Esquema Nacional de Seguridad (ENS), en particular MAGERIT y la norma UNE-ISO/IEC 27005, aplicable al sistema de información incluido en el alcance del SGSI.

Este análisis de riesgos se encuentra documentado, actualizado y almacenado en el repositorio corporativo de seguridad de la información, y sus resultados constituyen la base para la selección, implantación y seguimiento de las medidas de seguridad exigidas por el ENS.

La Declaración de Aplicabilidad (SoA) queda integrada en la herramienta oficial **INES** del **CCN-CERT**, que actualmente genera automáticamente la correspondencia de medidas ENS aplicables y su estado de implementación. Por este motivo, no se mantiene un documento SoA independiente.

Asimismo, la plataforma **INES** no permite todavía la incorporación directa del análisis de riesgos, quedando pendiente de integración con la herramienta **PILAR** según la planificación indicada por el **CCN-CERT**.

No obstante, el análisis de riesgos se encuentra plenamente disponible para su revisión durante auditorías internas, auditorías externas ENS y revisiones por la dirección.

El análisis de riesgos se revisa anualmente o cuando se produce cualquier cambio significativo en el sistema, en la tecnología utilizada, en los servicios soportados o en el contexto organizativo, dando cumplimiento al principio de mejora continúa establecido en el SGSI, la ISO 27001 y el ENS.

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.

LSH está vinculado al siguiente al siguiente **Marco Legislativo** y **Reglamentario** aplicable al sistema de información que da soporte al Servicio de Control Presencial:

- Legislación y Reglamentación Principal
- Constitución Española (CE) — Artículo 18 (protección de datos y secreto de las comunicaciones).
- Real Decreto 311/2022, por el que se regula el Esquema Nacional de Seguridad (ENS).
- Ley 40/2015, de Régimen Jurídico del Sector Público (art. 156 – ENS).
- Ley 39/2015, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Reglamento (UE) 2016/679, Reglamento General de Protección de Datos (RGPD).
- Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).
- Ley 34/2002, de servicios de la sociedad de la información y de comercio electrónico (LSSI).
- Ley 9/2014, General de Telecomunicaciones.
- Ley 6/2020, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Reglamento (UE) 910/2014 (eIDAS), relativo a la identificación electrónica y servicios de confianza.
- Real Decreto-ley 8/2019, sobre registro de jornada laboral (aplicable al control de presencia).
- Real Decreto Legislativo 1/1996, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual.

Este documento es CONFIDENCIAL y no se puede reproducir ni total ni parcialmente sin el consentimiento explícito y por escrito de NSC

Normativa del CCN-STIC aplicable al ENS

- Guías CCN-STIC aplicables al sistema (bastionado, Windows Server, criptografía, ENS, SaaS On-Premise, etc.).
- CPSTIC – Catálogo de Productos y Servicios de Seguridad TIC.

Para dar cumplimiento al marco penal en materia de seguridad, **LSH** asume como obligados los siguientes artículos del **Código Penal vigentes y aplicables a la seguridad de la información**:

- Delitos de descubrimiento y revelación de secretos: artículos 197 - 201.
- Delitos de estafa informática: artículos 248 - 251.
- Delitos de daños informáticos: artículos 264 - 264 ter.

Es responsabilidad de toda la organización de **LSH**, 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

Sabadell, a 2 de Diciembre de 2025

Este documento es CONFIDENCIAL y no se puede reproducir ni total ni parcialmente sin el consentimiento explícito y por escrito de NSC