POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Documento Interno

Código: PDS.01

Versión v.4 – 20/10/2026

Control de Cambios

Histórico de Cambios			
Versión	**Descripción del cambio**	**Autor**	**Fecha**
1	Primera edición del documento	LC	24/04/2023
2	Modificación general de la Política de seguridad para ser adaptada a la ISO/IEC 27001:2022	LC	23/09/2023
3	Actualización de la misión y los principios. Adaptación ENS. Adaptación a las nuevas oficinas.	LC	09/10/2026
4	Inclusión del uso de la IA	LC	20/10/2026

DERECHOS DE USO:

La presente documentación es propiedad de L4 Tech, S.L y tiene carácter confidencial. Por tanto, no podrá ser objeto de reproducción total o parcial, tratamiento informático ni transmisión de ninguna forma o por cualquier medio, ya sea electrónico, telemático, mecánico, por fotocopia, registro o cualquier otro. Así mismo tampoco podrá ser objeto de préstamo, alquiler o cualquier forma de cesión de uso sin el permiso previo y por escrito de L4 Tech, S.L, titular del copyright. El incumplimiento de las limitaciones señaladas por cualquier persona que tenga acceso a la documentación será perseguido conforme a ley.

L4 Tech, S.L.	info@level4.es
C/ Pere Cabrera 30	www.level4.es
25001 Lleida	Tel. (+34) 973 980 344

Índice de contenidos

Aprobación, alcance y misión 4
Marco normativo 4
Principios básicos 4
Uso de Inteligencia Artificial 4
Seguridad integral y mínimo privilegio 4
Supervisión, personal y mejora continua 4
Análisis y gestión de riesgos 5
Incidentes y defensa en profundidad 5
Control de accesos e instalaciones 5
Información, continuidad y trazabilidad 5
Productos, servicios y cumplimiento específico 5
Gobernanza y revisión 5
Protección de datos y documentación 6
Personal, incumplimientos y terceros 6

Aprobación, alcance y misión

Aprobada por la Dirección, esta política es de obligado cumplimiento para los servicios de soporte IT, cloud privado, backup, auditoría, desarrollo y compliance. Su finalidad es proteger los activos y la información, asegurar la continuidad de los servicios y reforzar la seguridad y el cumplimiento normativo de los clientes.

Marco normativo

Level4 aplica los requisitos de seguridad del Esquema Nacional de Seguridad (ENS), ISO/IEC 27001:2022 y la normativa aplicable sobre protección de datos y ciberseguridad, incluida NIS2 cuando corresponda. Los controles se adaptan a la sensibilidad de la información, la criticidad de los servicios y los riesgos identificados.

Principios básicos

La prevención comprende controles técnicos y organizativos, autorización previa de sistemas y evaluaciones periódicas. La detección exige supervisar los servicios y alertar sobre anomalías. Ante un incidente se activa su comunicación, evaluación y contención; la recuperación restablece la información y los servicios mediante copias de seguridad y medidas de continuidad.

Uso de Inteligencia Artificial

La inteligencia artificial solo debe utilizarse con fines legítimos, de forma segura y proporcionada. Antes de incorporar una herramienta o servicio de IA se evaluarán sus riesgos, la confidencialidad de los datos tratados, los accesos permitidos y la dependencia de proveedores. Se evitará introducir información sensible en herramientas no autorizadas y se preservará la trazabilidad de su uso.

Seguridad integral y mínimo privilegio

La seguridad comprende medidas técnicas, humanas, físicas, jurídicas y organizativas en todo el ciclo de vida de los sistemas. Se aplica el principio de mínimo privilegio: únicamente se habilitan las funciones, autorizaciones y accesos necesarios, eliminando servicios innecesarios y utilizando configuraciones seguras adaptadas al sistema.

Supervisión, personal y mejora continua

Se realiza una vigilancia permanente para detectar vulnerabilidades, configuraciones deficientes y desviaciones de seguridad. Los controles se revisan y mejoran periódicamente; el personal propio y externo recibe formación y supervisión, y los servicios de seguridad deben contar con profesionales cualificados.

Análisis y gestión de riesgos

El análisis y tratamiento de riesgos es una actividad continua, integrada en la gestión de seguridad. Las medidas de protección se seleccionan y justifican conforme al impacto y probabilidad de los riesgos, buscando mantenerlos en niveles aceptables y de forma proporcionada a los activos y servicios protegidos.

Incidentes y defensa en profundidad

Los incidentes se detectan, registran y clasifican según su impacto; se comunican al responsable de seguridad para coordinar la contención, el análisis, la recuperación y las medidas correctivas. La defensa en profundidad combina controles físicos, organizativos y técnicos para evitar que el fallo de una protección comprometa todo el sistema; las conexiones con otras redes se evalúan y protegen.

Control de accesos e instalaciones

La organización establece responsabilidades de seguridad diferenciadas y mecanismos formales de autorización. El acceso lógico se limita a usuarios, procesos, dispositivos y sistemas autorizados; las instalaciones se protegen mediante perímetros, controles de entrada y medidas frente a daños o accesos físicos indebidos.

Información, continuidad y trazabilidad

La información se protege tanto almacenada como durante su transmisión, incluidos dispositivos móviles, soportes y redes abiertas. Se mantienen copias de seguridad y medidas de recuperación y conservación; se registra la actividad necesaria para investigar accesos indebidos y se detecta código nocivo respetando la normativa de privacidad.

Productos, servicios y cumplimiento específico

Al adquirir soluciones o contratar servicios se comprueban la idoneidad de sus medidas de seguridad, las certificaciones pertinentes y la cualificación del proveedor. Se exige que las soluciones sean proporcionales al nivel de protección necesario y que las configuraciones eliminen funciones innecesarias. Los servicios compartidos e interconectados deben mantener controles equivalentes de seguridad.

Gobernanza y revisión

La Dirección aprueba esta política y designa los responsables de Organización, Servicios, Seguridad, Sistemas de Información, Protección de Datos y Gestión de la Seguridad. El Comité de Seguridad coordina su aplicación y revisión anual. Los nombramientos se formalizan por la Dirección y se revisan cada dos años o ante vacantes. Los conflictos se elevan al superior jerárquico y, si persisten, a la Dirección.

Protección de datos y documentación

Los datos personales se protegen mediante acceso restringido, tratamiento limitado a finalidades legítimas, conservación durante el tiempo necesario y medidas técnicas y organizativas adecuadas. Las reglas de seguridad son obligatorias; las tareas operativas deben describirse con claridad y las instrucciones técnicas deben permitir su ejecución segura. Toda documentación de seguridad debe mantenerse actualizada y accesible solo a personas autorizadas.

Personal, incumplimientos y terceros

Cada empleado debe utilizar los recursos de acuerdo con sus permisos, proteger la información y comunicar de inmediato incidentes o sospechas de riesgo. Recibirá formación de seguridad al menos una vez al año y formación específica antes de asumir funciones sensibles. Los incumplimientos pueden dar lugar a medidas disciplinarias. Los proveedores deben guardar confidencialidad, controlar los accesos, proteger sus equipos y notificar incidencias relacionadas con Level4.