Política de Seguridad, Continuidad y Resiliencia Digital

Publicación web

Sistema de Gestión de Seguridad de la Información, Continuidad y Resiliencia Digital

Versión	**1.1**
Clasificación	Público
Fecha	04/12/2025

1. INTRODUCCIÓN

Zertiban S.L.U. establece su compromiso firme con la seguridad de la información, la continuidad del negocio y la resiliencia digital, pilares fundamentales para garantizar la confianza de clientes, socios, proveedores y demás partes interesadas.

Esta política se basa en estándares internacionales y regulaciones europeas y nacionales de referencia, como ISO/IEC 27001, ISO 22301, el Esquema Nacional de Seguridad (ENS) y el Reglamento Europeo DORA (UE 2022/2554), asegurando un nivel de protección elevado frente a amenazas y riesgos tecnológicos.

La organización promueve una cultura de ciberseguridad activa, una gestión del riesgo proporcional y una mejora continua, con enfoque preventivo y correctivo.

El presente resumen expone los compromisos y medidas clave aplicables a los servicios prestados y a las relaciones con terceros, con impacto directo sobre la seguridad y calidad de los procesos digitales de Zertiban.

2. FUNDAMENTOS DE LA POLÍTICA

1. Compromiso institucional y liderazgo

- La Política de Seguridad, Continuidad y Resiliencia Digital está plenamente respaldada por la alta dirección y es aplicable a todo el personal de Zertiban y a terceros contratados.
- Su cumplimiento está supervisado por el Comité de Riesgos y Seguridad, con representación de roles clave como el CISO GRC (Chief Information Security Officer) y responsables de TIC, continuidad, protección de datos y proveedores.
- El Comité se encarga de impulsar las políticas, controlar su aplicación, asignar recursos y evaluar su eficacia periódicamente.

2. Cumplimiento normativo y alcance

- Esta política se alinea con las siguientes normas y marcos:
  - ENS (RD 311/2022) – Categoría ALTA.
  - ISO/IEC 27001:2022 – Gestión de la seguridad de la información.
  - ISO 22301:2019 – Continuidad del negocio.
  - Reglamento DORA (UE 2022/2554) – Resiliencia operativa digital.
  - Directiva NIS 2 (UE 2022/2555) – Ciberseguridad de redes y sistemas.
  - RGPD y LOPDGDD – Protección de datos personales.
- Se aplica a todas las operaciones, sistemas, personas y servicios de Zertiban, incluyendo servicios TIC críticos prestados a terceros del sector financiero o estratégico.

3. Gestión de riesgos y ciberresiliencia

- Zertiban aplica un enfoque basado en riesgos para proteger la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información.

- Se realizan análisis de riesgos anuales y ad hoc ante cambios o incidentes graves.
- Se contemplan los riesgos derivados de terceros o proveedores TIC críticos y se definen medidas proporcionadas a la criticidad de los activos.
- El análisis se realiza conforme al ENS, DORA y las mejores prácticas como NIST CSF o ISO 27005.

4. Seguridad por diseño y por defecto

- Todos los sistemas y servicios se configuran con principios de mínimo privilegio, segmentación de redes, y desactivación de funciones innecesarias.
- La asignación de accesos es controlada y documentada. El personal dispone de credenciales diferenciadas según roles.
- Se garantiza el registro de actividades y la trazabilidad de operaciones sensibles.

5. Protección de datos personales

- Zertiban asegura el cumplimiento del Reglamento General de Protección de Datos (RGPD) y la LOPDGDD, con apoyo de su Delegado de Protección de Datos (DPD).
- Se aplican medidas técnicas y organizativas adecuadas basadas en análisis de riesgos y, cuando corresponde, en evaluaciones de impacto (DPIA).
- Toda la información personal tratada se protege con medidas de seguridad equivalentes o superiores a las exigidas por el ENS y el DORA.

6. Continuidad del negocio y recuperación ante desastres

- Se han definido y documentado planes de:
  - Continuidad de negocio (BCP).
  - Recuperación ante desastres (DRP).
- Se establecen objetivos RTO y RPO para procesos críticos.
- Se realizan pruebas periódicas, simulacros y revisiones con participación de las unidades implicadas, con registro de resultados y acciones de mejora.

7. Gestión y notificación de incidentes

- Zertiban dispone de un procedimiento formal de gestión de incidentes TIC, alineado con ENS y DORA.
- Incluye:
  - Detección y escalado.
  - Comunicación interna y externa.
  - Medidas de contención y recuperación.
  - Notificación a autoridades competentes (CCN-CERT, supervisores financieros, AEPD…).
- Se analiza cada incidente para implementar mejoras que refuercen la ciberresiliencia de forma preventiva.

8. Relación con terceros y cadena de suministro TIC

- Los terceros que accedan a sistemas, datos o servicios de Zertiban deben adherirse a esta política.
- Se evalúan los riesgos derivados de terceros y se imponen obligaciones contractuales conforme al artículo 30 del Reglamento DORA:
  - Cláusulas de seguridad, auditoría, subcontratación, acceso a datos y rescisión.
  - Revisión periódica y, si aplica, auditorías a proveedores TIC críticos.

9. Formación, concienciación y cultura de seguridad

- Todos los empleados reciben formación inicial y continua en ciberseguridad, continuidad operativa y gestión de incidentes, al menos una vez al año.
- Se establece un programa específico para:
  - Nuevas incorporaciones.
  - Cambio de rol o funciones TIC.
  - Personal externo o de terceros relevantes.
- Se fomenta una cultura activa frente a amenazas como phishing, errores humanos o configuraciones inseguras.

10. Mejora continua y auditoría

- El sistema se revisa bajo el modelo PDCA (Planificar – Hacer – Verificar – Actuar).
- Se llevan a cabo:
  - Auditorías internas anuales.
  - Auditorías externas por parte de entidades independientes.
  - Auditorías extraordinarias en caso de cambios sustanciales o incidentes graves.
- Los resultados dan lugar a acciones correctivas y oportunidades de mejora, con seguimiento por el Comité de Riesgos y Seguridad.

Disponibilidad y revisión

- Este resumen forma parte de la política general, cuyo contenido completo está disponible bajo solicitud formal.
- La política se revisa al menos una vez al año o cuando existan cambios normativos, tecnológicos o estructurales relevantes.
- Todas las partes interesadas pueden remitir dudas o sugerencias a través del canal oficial de cumplimiento y seguridad de Zertiban.