Política de seguridad de la información

TRES BITS INGENIEROS DE SOFTWARE SL

ANEXO 01 | Versión 2 | Fecha 07/11/2026

1 Misión y alcance

TresBits diseña, desarrolla, implanta y da soporte a soluciones de software. La seguridad de la información protege la prestación de estos servicios, la información propia y de clientes y la continuidad de la actividad. Esta política establece las directrices de Dirección y el marco para los objetivos del Sistema de Gestión de Seguridad de la Información, integrado con ISO 27001 y el Esquema Nacional de Seguridad.

Se aplica a los sistemas de información que soportan los procesos de diseño, desarrollo, implantación y soporte de soluciones de software, al personal y a los proveedores que intervienen en ellos. Comprende la infraestructura propia o contratada y los accesos a infraestructura de clientes necesarios para prestar los servicios. La descripción del sistema, los contratos y los inventarios concretan los límites y responsabilidades de cada servicio.

2 Compromiso de Dirección

Dirección proporciona autoridad y recursos para gestionar la seguridad, cumplir los requisitos aplicables y mejorar continuamente. Los objetivos deben ser medibles, disponer de responsables y plazos y evaluarse mediante indicadores y evidencias. La seguridad se integra en las decisiones de negocio, la contratación y el ciclo de vida de los servicios.

- Proteger la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información y los servicios según sus necesidades y riesgos.
- Gestionar la seguridad como un proceso integral, basado en riesgos, con medidas de prevención, detección, respuesta, conservación y recuperación.
- Establecer líneas de defensa, mínimo privilegio, configuración segura y diferenciación de responsabilidades.
- Mantener vigilancia continua, reevaluar las medidas y promover formación y concienciación del personal.
- Preservar la continuidad del negocio y mejorar los servicios mediante seguimiento, auditorías, acciones correctivas y revisión por Dirección.

3 Marco normativo y contractual

Son referencias el Real Decreto 311/2022 por el que se regula el ENS, sus instrucciones técnicas de seguridad aplicables, el Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018 en materia de datos personales, así como la legislación, contratos y requisitos de los clientes que resulten aplicables a cada servicio. ISO/IEC 27001 constituye el marco del SGSI. Las guías CCN-STIC se utilizan como apoyo técnico. ANEXO 06 relaciona la normativa externa aplicable.

4 Organización de la seguridad

Rol	Designación
Dirección y responsables de información y servicio	Persona designada en ACTA CS 2026 01
Responsable de Seguridad	Persona designada en ACTA CS 2026 01
Adjunto al Responsable de Seguridad	Persona designada en ACTA CS 2026 01
Responsable del sistema	Persona designada en ACTA CS 2026 01

El responsable de la información determina sus necesidades de protección y clasificación. El responsable del servicio determina los requisitos de prestación, disponibilidad y recuperación. Ambos consideran los requisitos contractuales y las decisiones de los clientes sobre su información y servicios. La responsabilidad última de las entidades públicas destinatarias se mantiene en sus respectivos ámbitos.

El Responsable de Seguridad determina las medidas para satisfacer esos requisitos, supervisa su implantación y eficacia, coordina riesgos e incidentes y reporta a Dirección. Puede exigir actuaciones y evidencias a los responsables técnicos, solicitar asesoramiento y escalar incumplimientos. Actúa como punto de contacto de seguridad con los clientes y terceros. El Adjunto al Responsable de Seguridad apoya de forma habitual la supervisión y el seguimiento de las actuaciones de seguridad. Durante la ausencia o impedimento del Responsable de Seguridad asume sus funciones, dejando constancia del inicio y fin de la sustitución. El apoyo habitual no duplica la titularidad ni altera la diferenciación respecto del Responsable del Sistema.

El Responsable del Sistema dirige la operación diaria y la implantación técnica de las medidas, coordinando administradores, responsables de activos y proveedores. Propone soluciones, mantiene la configuración y aporta las evidencias de ejecución.

La supervisión de seguridad y la operación del sistema son funciones diferenciadas. El Responsable de Seguridad reporta directamente a Dirección y actúa con independencia funcional respecto del Responsable del Sistema. Ninguno de estos roles dirige las decisiones del otro dentro de su función ENS. Los desacuerdos se documentan y se elevan a Dirección y al Comité de Seguridad, sin dispensar el cumplimiento de requisitos obligatorios.

5 Comité de Seguridad

El Comité está compuesto por Dirección, que lo preside, el Responsable de Seguridad, que coordina sus trabajos y custodia las actas, el Responsable del Sistema y el Adjunto al Responsable de Seguridad. El Adjunto apoya el seguimiento y solo ejerce la titularidad de seguridad durante la sustitución registrada. Podrán participar responsables de proyectos, protección de datos, proveedores o especialistas cuando el asunto lo requiera. ACTA CS 2026 01 identifica a las personas designadas y su aceptación.

El Comité coordina la seguridad, revisa riesgos, incidentes, vulnerabilidades, indicadores, auditorías y planes de mejora, y propone prioridades y recursos. Dirección conserva la aprobación de la política y las decisiones de negocio y recursos. Las decisiones de aceptación de riesgo corresponden a quienes tienen responsabilidad sobre la información y el servicio afectados, con asesoramiento de seguridad y respeto a los requisitos obligatorios.

Se reunirá al menos trimestralmente y de forma extraordinaria ante incidentes graves, cambios relevantes o discrepancias que lo requieran. Los acuerdos identificarán responsables, plazos y evidencias de seguimiento. Se procurará el consenso y los asuntos no resueltos se elevarán a Dirección con las posiciones y riesgos documentados.

6 Designación y competencias

Dirección designa por escrito a los titulares de cada rol y a sus sustitutos, define su ámbito y autoridad y comunica las funciones. Las designaciones se revisan anualmente y cuando cambian las personas, el alcance o la estructura. La renovación, sustitución o cese se registra y conlleva la revisión de accesos y delegaciones. Dirección asegura tiempo, recursos y competencia suficientes, con formación y asesoramiento técnico cuando sean necesarios.

7 Gestión de riesgos y protección de datos

La categorización del sistema se basa en la valoración de las cinco dimensiones de seguridad. El análisis de riesgos identifica activos, amenazas, salvaguardas y riesgos residuales y utiliza una metodología coherente con el ENS. Las decisiones de tratamiento, responsables, recursos y estado de implantación se registran y se relacionan con la Declaración de Aplicabilidad ENS y el SGSI.

Los tratamientos de datos personales incorporan los requisitos del responsable o del encargado del tratamiento, la privacidad desde el diseño y por defecto y el análisis de riesgos para los derechos y libertades de las personas. Se realiza evaluación de impacto cuando resulte exigible. El rol de protección de datos del SGSI asesora en su ámbito y coordina con seguridad las brechas y comunicaciones correspondientes, con el asesoramiento del DPD cuando proceda.

8 Directrices operativas y de proveedores

Se mantendrán inventarios actualizados, accesos autorizados y revisados, protección de credenciales, configuración y actualización seguras y tratamiento de vulnerabilidades. El desarrollo y los cambios deberán incorporar revisión, validación, autorización y trazabilidad proporcionadas al riesgo.

Los procedimientos definirán copias, pruebas de recuperación, gestión de incidentes y continuidad según los requisitos de cada servicio. Los acuerdos con proveedores concretarán responsabilidades, accesos, medidas, seguimiento y comunicación de incidentes. Las certificaciones de los proveedores se comprobarán respecto del servicio contratado. El personal comunicará sin demora las sospechas, incidentes e incumplimientos por los canales establecidos.

9 Documentación y comunicación

La documentación se estructura en política, normativa, procedimientos e instrucciones y registros o evidencias. El Manual de Funciones (ANEXO 02) desarrolla la organización y ACTA CS 2026 01 identifica a las personas designadas y su aceptación. El control documental del SGSI regula elaboración, aprobación, acceso, distribución, conservación y retirada de documentos. La documentación se protege según su clasificación y se publica o comunica en función de sus destinatarios.

Esta política se comunica a todo el personal y a los terceros afectados. El conocimiento de las obligaciones se respalda con registros de comunicación y formación. La información pública de seguridad se facilita sin divulgar configuraciones sensibles, credenciales ni datos personales innecesarios.

10 Revisión y aprobación

Dirección revisará esta política al menos anualmente y ante cambios relevantes, incidentes o resultados de auditoría que lo aconsejen. Su aprobación se formaliza mediante la firma de Dirección y ACTA CS 2026 01 del Comité de Seguridad.

Aprobación por Dirección
José Cifre Broseta, Dirección
Fecha: 09/11/2026

52655184L JOSE MANUEL CIFRE (R: B98578966)

Firmado digitalmente por 52655184L JOSE MANUEL CIFRE (R: B98578966)
Fecha: 2026.11.09 08:14:32 +01'00'