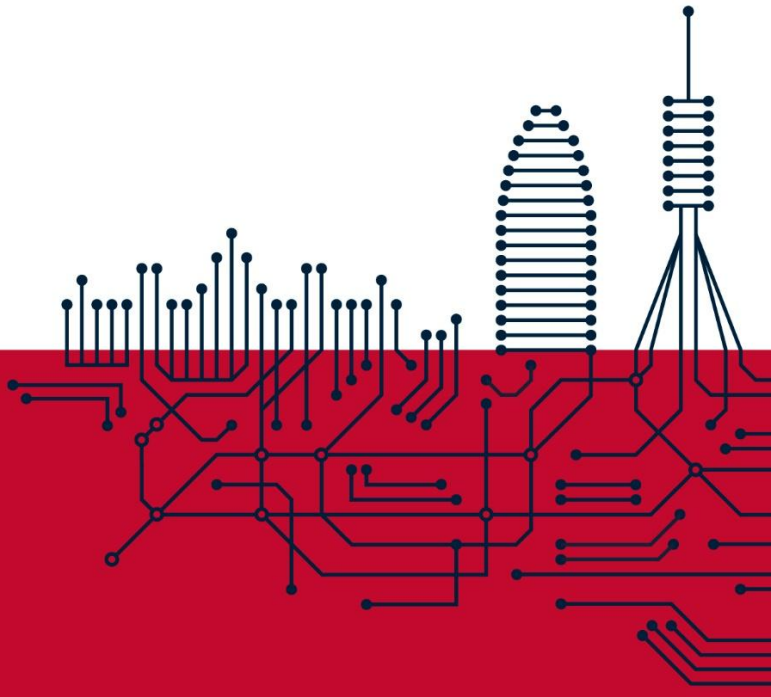
Smarting
ENGINEERING



Política
Seguridad de la Información

SGSI.PR.01.es v1.2

31/03/2026

1. Declaración de la Dirección

En **Smarting**, la confidencialidad, integridad y disponibilidad de la información que tratamos —propia, de nuestros clientes y de nuestros usuarios— son elementos estratégicos para garantizar la confianza, el cumplimiento normativo y la sostenibilidad del negocio.

La Dirección de **Smarting Engineering, S.L.** declara su compromiso con el establecimiento, implementación, mantenimiento y mejora continua del **Sistema de Gestión de Seguridad de la Información (SGSI)**, alineado con los estándares ISO/IEC 27001:2022, el Esquema Nacional de Seguridad (ENS, RD 311/2022) en categoría MEDIA, y complementado por el Sistema de Gestión de Continuidad del Negocio (SGCN) basado en ISO 22301:2019.

La Dirección asume los siguientes compromisos:

1.1. Apropiada al propósito de la organización

- **Smarting** desarrolla soluciones digitales y presta soporte operativo a clientes y proveedores, siendo la plataforma Motorcloud y los servicios asociados los activos esenciales de la organización.
- Proteger la **confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad** de la información manejada en el **desarrollo de soluciones**, la prestación de servicios y el **soporte a clientes institucionales**.
- Integrar la seguridad de la información en todos los procesos de negocio, desde el diseño y desarrollo hasta la operación y el soporte.
- Mantener la confianza de nuestros clientes, en particular de las **autoridades de transporte y operadores** que confían en nuestros servicios.

1.2. Marco de referencia para los objetivos de seguridad

Esta política proporciona el marco para establecer **objetivos medibles** de seguridad de la información, alineados con la dirección estratégica de la organización. Los objetivos se concretan anualmente en la Revisión por la Dirección y cumplen el criterio SMART.

- **RTO** (Recovery Time Objective): tiempos objetivo de recuperación de los servicios críticos.
- **RPO** (Recovery Point Objective): pérdida máxima de datos aceptable.
- Maduración operativa: **MTTD, MTTR, cobertura de backups 3-2-1**, consolidación del SIEM y EDR.
- Certificación normativa: mantenimiento de ENS MEDIA e ISO 27001, certificación ISO 22301 y preparación hacia ENS Categoría Alta.

1.3. Compromiso de cumplir los requisitos aplicables

Cumplir con todos los **requisitos legales, regulatorios, contractuales y normativos** aplicables a la seguridad de la información, incluyendo:

- **ISO/IEC 27001:2022** y los controles del Anexo A.
- **ENS (RD 311/2022)** en categoría MEDIA, con orientación hacia categoría Alta.
- **RGPD / LOPDGDD** en materia de protección de datos personales.
- **ISO 22301:2019** como referencia para la continuidad del negocio.

- **Directiva NIS2** como referencia para la preparación de la organización ante futuras obligaciones.
- **Requisitos contractuales** con clientes, especialmente con la Autoritat del Transport Metropolità de Barcelona (ATM).

Proporcionar los **recursos necesarios** (humanos, técnicos, formativos y económicos) para el establecimiento, implementación y mejora continua del SGSI.

1.4. Compromiso de mejora continua del SGSI

Promover la **mejora continua** del SGSI mediante:

- **Análisis y gestión de riesgos** periódica con metodología MAGERIT.
- **Auditorías internas y externas** anuales (ENS, ISO 27001) y pruebas de seguridad (pentesting).
- **Revisión por la Dirección** anual conforme a la cláusula 9.3 de la norma.
- **Gestión de no conformidades y acciones correctivas** trazada en YouTrack.
- **Integración de lecciones aprendidas** de incidentes y simulacros.

Promover una **cultura de seguridad** mediante formación periódica y sensibilización de todo el personal, garantizando la adaptabilidad del SGSI a los cambios tecnológicos, organizativos, regulatorios y del entorno de amenazas.

2. Alcance

Esta política aplica a todos los **procesos, recursos, tecnologías, infraestructuras y personas** incluidos en el alcance del SGSI, así como a proveedores y terceros que puedan impactar en la seguridad de la información de Smarting. Esto incluye:

- El **desarrollo de soluciones digitales** de Smarting, incluyendo la plataforma Motorcloud y sus servicios.
- La **operación de los servicios** prestados a clientes y proveedores.
- La **infraestructura tecnológica** asociada (centros de datos, redes, sistemas y plataformas).
- Todo el **personal** de Smarting, con independencia de su régimen contractual o ubicación.
- Los **proveedores y terceros críticos** que tratan información de Smarting o de sus clientes.

3. Marco Organizativo de la Seguridad

Smarting ha identificado y definido los roles y funciones de seguridad necesarios para garantizar la protección de la información, conforme al capítulo II del **Real Decreto 311/2022** y la cláusula 5.3 de ISO 27001:2022.

3.1. Comité de Seguridad

Smarting ha constituido un **Comité de Seguridad** que supervisa el cumplimiento del SGSI y del SGCN. Sus funciones son:

- Coordinar todas las actividades relacionadas con la seguridad de la información y la continuidad del negocio.
- Proponer y revisar la Política de Seguridad y la Política de Continuidad.
- Aprobar las normas, procedimientos y requisitos de formación en materia de seguridad.
- Supervisar la gestión de incidentes, no conformidades y acciones correctivas.

- Evaluar la activación de los planes de continuidad ante disrupciones.

3.2. Roles principales

Los nombramientos de **CISO**, **Responsable del Servicio (RE)** y **DPO** son aprobados por la Dirección a propuesta del Comité de Seguridad y se revisan cada dos años o cuando el puesto quede vacante. La función de Responsable de la Información (**CIO**) recae en el **CTO**.

3.3. Resolución de conflictos

Smarting ha definido el proceso y jerarquía para la **resolución de conflictos de autoridad** entre los perfiles críticos con responsabilidades en seguridad, aplicable a todos los perfiles del SGSI y del SGCN.

4. Análisis y Gestión de Riesgos

Todos los sistemas sujetos a esta política se evalúan mediante un **análisis de riesgos** basado en metodología **MAGERIT**, valorando amenazas, vulnerabilidades e impactos. Este análisis se repite:

- Regularmente, al menos una vez al año.
- Cuando cambie la información manejada.
- Cuando cambien los servicios prestados.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

5. Categorización de los Sistemas

Smarting clasifica sus sistemas conforme al Anexo II del ENS en categorías **Básica, Media o Alta**, en función del nivel más alto de las dimensiones de seguridad valoradas (confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad).

El proceso de categorización contempla la identificación de sistemas y activos críticos, la evaluación del valor de la información (incluyendo categorías especiales del RGPD), el análisis de riesgos, el cumplimiento normativo, la dependencia entre sistemas, los requisitos de las dimensiones de seguridad y la capacidad de recuperación. Cuando un cliente determine una categorización propia, **prevalecerá la categoría establecida por el cliente**.

6. Gestión del Personal y Profesionalidad

Todos los miembros de **Smarting** tienen la **obligación de conocer y cumplir** esta política y la Normativa de Seguridad. El Comité de Seguridad es responsable de aplicar las medidas necesarias para que la información llegue a los afectados.

Todos los empleados reciben **sesiones de concienciación** en materia de seguridad al menos una vez al año, complementadas con un programa de concienciación continua y formación específica para nuevas incorporaciones.

El personal dedicado a tareas de seguridad cuenta con la **cualificación apropiada** y recibe la formación específica necesaria para garantizar la seguridad de las tecnologías de la información en todas las fases del ciclo de vida.

Los mismos requisitos se exigen a los proveedores que prestan servicios relacionados con la seguridad, mediante un procedimiento formal de evaluación de proveedores.

7. Autorización y Control de los Accesos

Los sistemas de información de **Smarting** cuentan con mecanismos formales de **autorización, autenticación y trazabilidad** que permiten conceder, denegar o revocar accesos cuando es necesario. El acceso se limita a lo estrictamente necesario para el desempeño de las funciones de cada persona o sistema.

8. Protección de las Instalaciones

Las instalaciones de **Smarting** están protegidas frente a daños que puedan afectar a los sistemas que albergan y frente a accesos de personas no autorizadas, conforme a los procedimientos vigentes de protección de instalaciones e infraestructuras.

9. Adquisición de Productos y Servicios de Seguridad

Toda nueva adquisición de **producto o servicio de seguridad** que pueda afectar al SGSI se evalúa previamente desde el punto de vista funcional y de requisitos de seguridad. La validación incluye prueba formal del producto y comprobación de cumplimiento.

Los productos de seguridad se priorizan conforme al **Catálogo CPSTIC (CCN-STIC 105)**. Cuando no existe alternativa CPSTIC adecuada, se aplica un procedimiento formal de justificación, validación y aprobación por el Comité de Seguridad.

Todo servicio contratado se evalúa antes de su puesta en producción para asegurar el cumplimiento de los requisitos mínimos de seguridad definidos en esta política y en la Normativa de Seguridad.

10. Principio de Mínimo Privilegio

El SGSI de **Smarting** aplica el **Principio del Mínimo Privilegio**: a cada usuario, proceso, aplicación o dispositivo se le otorgan únicamente los permisos estrictamente necesarios para desempeñar sus funciones legítimas.

Este principio reduce la exposición a ciberataques y previene la acumulación indebida de privilegios, aplicándose tanto a usuarios humanos como a aplicaciones, sistemas o dispositivos conectados que requieren privilegios para realizar tareas necesarias.

11. Integridad y Actualización del Sistema

Cualquier **cambio físico o lógico** sobre los sistemas de información se realiza únicamente tras su aprobación formal y siguiendo un procedimiento documentado.

Las actualizaciones, parches y cambios en especificaciones se analizan para evitar la degradación de la seguridad y se gestionan los riesgos introducidos por los cambios.

12. Protección de la Información Almacenada y en Tránsito

La información debe estar protegida durante todo su **ciclo de vida**, tanto en almacenamiento como en transmisión, en soporte electrónico y físico. Se aplican procedimientos específicos para el manejo, etiquetado, tratamiento y eliminación segura de la información.

13. Prevención ante Sistemas Interconectados

Las conexiones con sistemas de información externos se realizan con medidas de **protección perimetral, control de accesos y registro de actividad** para detectar anomalías. Las conexiones siguen las directrices de las guías **CCN-STIC** publicadas al efecto.

14. Registro de Actividad y Detección de Código Dañino

Smarting supervisa sus sistemas de información mediante **SIEM y herramientas EDR**, registrando eventos relevantes como incidencias de seguridad. La supervisión respeta los requisitos legales de privacidad y se utiliza para verificar la eficacia de los controles y el cumplimiento de la política de control de accesos.

Todos los equipos corporativos disponen de **herramientas antivirus de última generación (EDR)** con gestión centralizada para la protección, detección, recuperación y eliminación de código malicioso.

La gestión de incidentes se trazea en **YouTrack** conforme a la taxonomía **CCN-STIC 817**, con notificación a las autoridades competentes (CCN-CERT, AEPD, INCIBE) cuando corresponda.

15. Gestión de Incidentes de Seguridad

La Dirección de **Smarting** ha establecido un **procedimiento formal de notificación** de incidentes de seguridad. Todo el personal debe notificar incidencias mediante el canal habilitado (**security@smarting.es**) de forma inmediata. Esto garantiza una respuesta rápida y efectiva ante incidencias y debilidades.

16. Continuidad de la Actividad

Smarting dispone de un **Sistema de Gestión de Continuidad del Negocio (SGCN)** basado en **ISO 22301:2019** que complementa el SGSI. El SGCN garantiza la capacidad de la organización para mantener los servicios esenciales y recuperarse frente a disrupciones, mediante:

- Un **Análisis de Impacto en el Negocio (BIA)** que identifica procesos críticos y tiempos de recuperación.
- Un **Plan de Continuidad del Negocio (BCP)** que coordina la respuesta operativa.
- **Planes Tecnológicos de Recuperación (DRP)** que cubren la restauración de la infraestructura.
- **Pruebas periódicas y simulacros** que validan la eficacia de los planes.

La gestión de la continuidad se rige por su política específica, definida en la **Política de Continuidad del Negocio** (SGCN.PR.01.es), que complementa el presente apartado.

17. Mejora Continua del SGSI

La Dirección se compromete a **desarrollar, implantar, mantener y mejorar continuamente** la presente Política y su Sistema de Gestión, valorando especialmente la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información crítica.

La mejora continua se articula mediante **auditorías, revisiones por la dirección, análisis de indicadores, gestión de no conformidades** y la integración de lecciones aprendidas de incidentes y ejercicios.

18. Datos de Carácter Personal

Smarting trata datos de carácter personal cumpliendo el **RGPD** y la **LOPDGDD**. Considerando el estado de la técnica, los costes, la naturaleza y los riesgos del tratamiento, **Smarting** ha aplicado medidas técnicas y organizativas apropiadas, entre otras:

- Seudonimización y cifrado de datos personales.
- Capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas de tratamiento.
- Capacidad de restaurar la disponibilidad y el acceso a los datos personales rápidamente en caso de incidente físico o técnico.
- Procesos de verificación, evaluación y valoración regulares de la eficacia de las medidas.

La supervisión del tratamiento de datos personales recae en la figura del **DPO**, designado conforme al RGPD.

19. Estructuración de la Documentación de Seguridad

La documentación de seguridad sigue las directrices establecidas en los procedimientos de control documental, con medidas para estructurar, gestionar y controlar el acceso a la documentación, garantizando su integridad y confidencialidad.

La documentación se gestiona en la **Base de Conocimiento corporativa**, con control de versiones, trazabilidad de cambios y acceso restringido a personal autorizado: miembros del Comité de Seguridad, representantes del cliente y consultores o auditores autorizados.

20. Documentación y Comunicación

Esta política cumple con los requisitos de comunicación establecidos en ISO 27001 (5.2):

Requisito	Cómo se cumple
a) Información documentada	Política versionada con control de cambios. Copia firmada en el archivo de seguridad.
b) Comunicada dentro de la organización	Sesiones de formación y concienciación. Canal Teams ENS-ISO. Base de conocimiento accesible a todo el personal.
c) Disponible para partes interesadas	Publicada en la web corporativa de Smarting en tres idiomas (ES, CA, EN). Disponible bajo petición para clientes y auditores.

21. Revisión y Actualización

Esta política se revisa **anualmente** como parte de la Revisión por la Dirección. Se revisa **anticipadamente** cuando se producen:

- Cambios significativos en los servicios, la infraestructura o la estructura organizativa.
- Nuevos requisitos legales, regulatorios o contractuales.
- Lecciones aprendidas de incidentes o ejercicios que requieran ajustes en los compromisos.
- Cambios significativos en el entorno de amenazas o en el contexto del negocio.

La revisión se documenta en las actas del Comité de Seguridad y en la Revisión por la Dirección.

22. Aprobación

Mediante la aprobación de esta política, la Dirección de **Smarting Engineering, S.L.** manifiesta su determinación y compromiso en alcanzar un nivel de seguridad adecuado a las necesidades del negocio, garantizando la protección de la información, los servicios y las personas de forma integrada y coherente con el SGCN.

Aprobado por:	Dirección de **Smarting Engineering, S.L.**
Fecha:	31/03/2026
Firma:	La Dirección

Nota: Los documentos mencionados en la presente política son de actualización periódica y se encuentran disponibles para su consulta por las partes interesadas. Pueden solicitarse a **security@smarting.es**