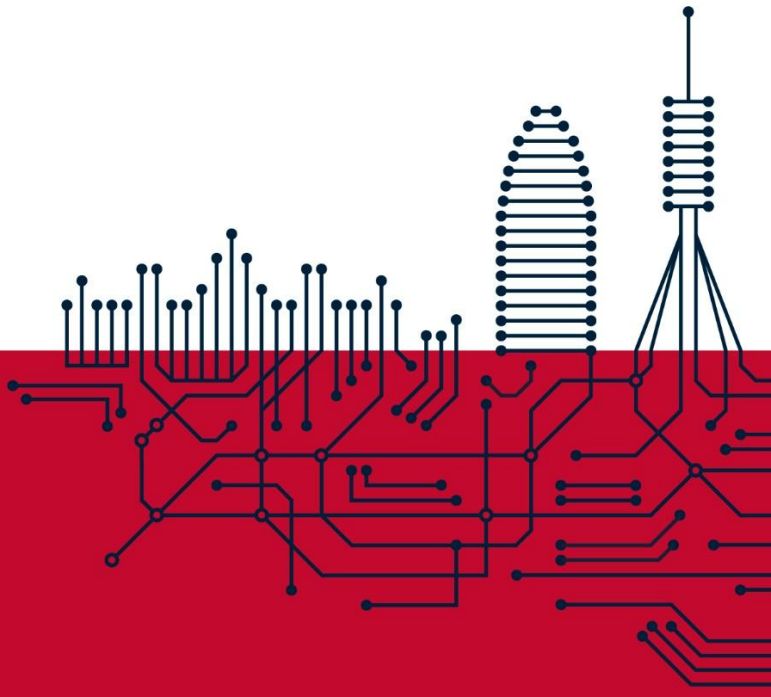
Smarting
ENGINEERING



Política
Continuidad del Negocio

SGCN.PR.01.es v1.1

06/03/2026

1. Declaración de la Dirección

En **Smarting**, la continuidad de los servicios críticos y la resiliencia organizativa son elementos estratégicos para garantizar la confianza de nuestros clientes, socios, usuarios y partes interesadas.

La Dirección de **Smarting Engineering, S.L.** declara su compromiso con el establecimiento, implementación, mantenimiento y mejora continua del **Sistema de Gestión de Continuidad del Negocio (SGCN)**, y asume los siguientes compromisos:

1.1. Apropiada al propósito de la organización

- Mantener la **disponibilidad de la plataforma Motorcloud**, los servicios prestados a través de ella y el soporte a clientes y proveedores, como actividad esencial de **Smarting**.
- Proteger la capacidad de **Smarting** para **entregar productos y servicios** a sus clientes dentro de **plazos aceptables** y a una **capacidad predefinida** durante una disrupción.
- Integrar la gestión de continuidad en todos los procesos de negocio, desde el desarrollo de soluciones hasta la operación y el soporte.

1.2. Marco de referencia para objetivos de continuidad

Esta política proporciona el marco para establecer **objetivos medibles** de continuidad del negocio, incluyendo:

- **RTO** (Recovery Time Objective): tiempo objetivo de recuperación de cada servicio crítico.
- **RPO** (Recovery Point Objective): pérdida máxima de datos aceptable.
- **MTPD** (Maximum Tolerable Period of Disruption): periodo máximo de interrupción tolerable.

Los objetivos concretos se definen en los Objetivos de Continuidad (cont.3.2), con base en los resultados del Análisis de Impacto en el Negocio (BIA, cont.5.1).

La organización prioriza los servicios y procesos esenciales para asegurar la recuperación dentro de los plazos establecidos, y coordina la respuesta de todas las áreas mediante planes específicos (BCP, Protocolo de Emergencia, Medios Alternativos).

1.3. Compromiso de cumplir los requisitos aplicables

Cumplir con todos los **requisitos legales, regulatorios, contractuales y normativos** aplicables a la continuidad del negocio, incluyendo:

- **UNE-EN ISO 22301:2020** — Sistema de Gestión de la Continuidad del Negocio.
- **ISO/IEC 27001:2022** — Controles de continuidad de la seguridad de la información.
- **ENS (RD 311/2022)** — Medidas de continuidad del servicio (op.cont) en categoría media.
- **RGPD / LOPDGDD** — Disponibilidad y recuperación de datos personales.
- **Requisitos contractuales** con clientes, especialmente con la Autoritat del Transport Metropolità de Barcelona (ATM).

Proporcionar los **recursos necesarios** para el establecimiento, implementación y mejora continua del SGCN.

1.4. Compromiso de mejora continua del SGCN

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

- **Pruebas periódicas y simulacros** que validen la eficacia de los planes.
- **Auditorías internas** que verifiquen el cumplimiento de los requisitos.
- **Revisiones por la Dirección** que evalúen el desempeño y orienten las decisiones.
- **Gestión de no conformidades y acciones correctivas** que eliminen las causas de las desviaciones.
- Integración de las **lecciones aprendidas** de incidentes reales y ejercicios.

Promover una **cultura de prevención y respuesta eficaz** frente a incidentes y desastres en toda la organización.

Garantizar la **protección de la vida, la información y la reputación corporativa** en escenarios de disrupción.

2. Alcance

La política aplica a todos los **procesos, recursos, tecnologías e infraestructuras** de **Smarting** incluidos en el alcance del SGCN (cont.1.3), así como a **proveedores y terceros críticos** que puedan impactar en la continuidad de los servicios.

Esto incluye, sin limitarse a:

- La **plataforma Motorcloud** y todos los servicios en producción.
- Los **dos centros de datos** y la infraestructura asociada.
- Los equipos de **explotación, desarrollo, sistemas y soporte**.
- Los **proveedores críticos** de infraestructura, telecomunicaciones y servicios.

3. Responsabilidades

La siguiente tabla resume las responsabilidades respecto a esta política:

Rol	Responsabilidad respecto a esta política
Dirección	Aprobar la política y asignar los recursos necesarios para su cumplimiento.
CISO	Mantener la política actualizada, coordinar su integración con el SGSI y difundirla.
Comité de Seguridad	Supervisar el cumplimiento de la política y evaluar la activación de los planes de continuidad.
Responsables de Áreas Críticas	Asegurar que sus equipos conocen y aplican la política en su ámbito.
Todos los empleados	Conocer sus funciones dentro del BCP, participar en la formación y pruebas de continuidad, y reportar incidentes.

4. Comunicación y Disponibilidad

Esta política cumple con los requisitos de comunicación establecidos en ISO 22301 (5.2.2):

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.

5. Revisión

- Esta política se revisará **anualmente** como parte de la Revisión por la Dirección.
- Se revisará **anticipadamente** cuando se produzcan:
  - 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.
- La revisión se documentará en las actas del Comité de Seguridad y en el Registro de cambios (cont.3.3).

6. Relación con la Política de Seguridad

Esta política complementa el apartado 16 (Continuidad de la actividad) de la **Política de Seguridad de la Información** (SGSI.PR.01.es) de **Smarting**. Ambas políticas comparten la estructura de gobierno del Comité de Seguridad y se gestionan de forma integrada.

7. Aprobación

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

Aprobado por:	Dirección de **Smarting Engineering, S.L.**
Fecha:	06/03/2026
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**