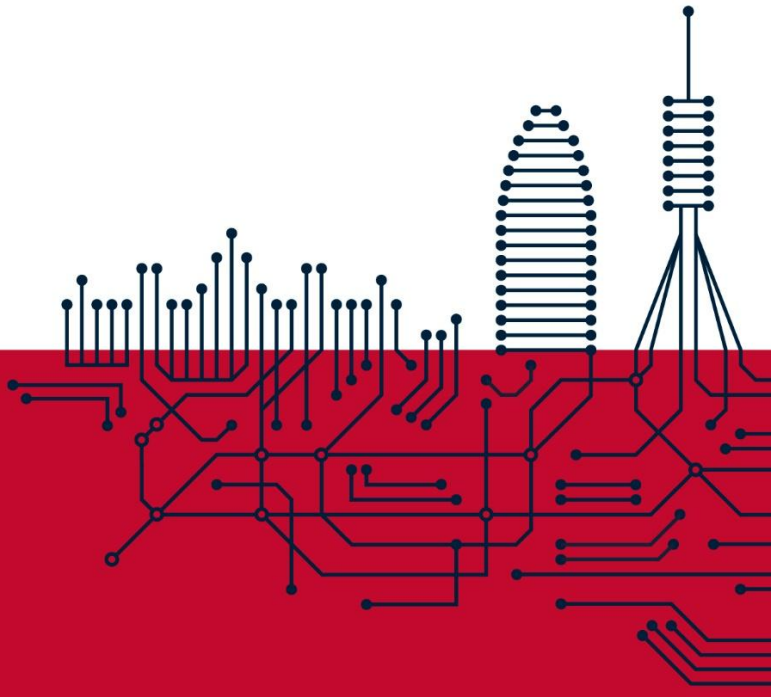
Smarting
ENGINEERING



Política
Continuïtat del Negoci

SGCN.PR.01.ca v1.1

06/03/2026

1. Declaració de la Direcció

A **Smarting**, la continuïtat dels serveis crítics i la resiliència organitzativa són elements estratègics per garantir la confiança dels nostres clients, socis, usuaris i parts interessades.

La Direcció de **Smarting Engineering, S.L.** declara el seu compromís amb l'establiment, implementació, manteniment i millora contínua del **Sistema de Gestió de Continuïtat del Negoci (SGCN)**, i assumeix els compromisos següents:

1.1. Apropiada al propòsit de l'organització

- Mantenir la **disponibilitat de la plataforma Motorcloud**, els serveis prestats a través d'ella i el suport a clients i proveïdors, com a activitat essencial de **Smarting**.
- Protegir la capacitat de **Smarting** per **lliurar productes i serveis** als seus clients dins de **terminis acceptables** i a una **capacitat predefinida** durant una disrupció.
- Integrar la gestió de continuïtat en tots els processos de negoci, des del desenvolupament de solucions fins a l'operació i el suport.

1.2. Marc de referència per a objectius de continuïtat

Aquesta política proporciona el marc per establir **objectius mesurables** de continuïtat del negoci, incloent-hi:

- **RTO** (Recovery Time Objective): temps objectiu de recuperació de cada servei crític.
- **RPO** (Recovery Point Objective): pèrdua màxima de dades acceptable.
- **MTPD** (Maximum Tolerable Period of Disruption): període màxim d'interrupció tolerable.

Els objectius concrets es defineixen en els Objectius de Continuïtat (cont.3.2), sobre la base dels resultats de l'Anàlisi d'Impacte en el Negoci (BIA, cont.5.1).

L'organització prioritza els serveis i processos essencials per assegurar la recuperació dins dels terminis establerts, i coordina la resposta de totes les àrees mitjançant plans específics (BCP, Protocol d'Emergència, Mitjans Alternatius).

1.3. Compromís de complir els requisits aplicables

Complir amb tots els **requisits legals, reguladors, contractuals i normatius** aplicables a la continuïtat del negoci, incloent-hi:

- **UNE-EN ISO 22301:2020** — Sistema de Gestió de la Continuïtat del Negoci.
- **ISO/IEC 27001:2022** — Controls de continuïtat de la seguretat de la informació.
- **ENS (RD 311/2022)** — Mesures de continuïtat del servei (op.cont) en categoria mitjana.
- **RGPD / LOPDGDD** — Disponibilitat i recuperació de dades personals.
- **Requisits contractuals** amb clients, especialment amb l'Autoritat del Transport Metropolità de Barcelona (ATM).

Proporcionar els **recursos necessaris** per a l'establiment, implementació i millora contínua del SGCN.

1.4. Compromís de millora contínua del SGCN

Promoure la **millora contínua** del SGCN mitjançant:

- **Proves periòdiques i simulacres** que validin l'eficàcia dels plans.
- **Auditories internes** que verifiquin el compliment dels requisits.
- **Revisions per la Direcció** que avaluïn l'acompliment i orientin les decisions.
- **Gestió de no conformitats i accions correctives** que eliminin les causes de les desviacions.
- Integració de les **lliçons apreses** d'incidents reals i exercicis.

Promoure una **cultura de prevenció i resposta eficaç** davant d'incidents i desastres en tota l'organització.

Garantir la **protecció de la vida, la informació i la reputació corporativa** en escenaris de disrupció.

2. Abast

La política s'aplica a tots els **processos, recursos, tecnologies i infraestructures** de **Smarting** inclosos en l'abast del SGCN (cont.1.3), així com a **proveïdors i tercers crítics** que puguin impactar en la continuïtat dels serveis.

Això inclou, sense limitar-se a:

- La **plataforma Motorcloud** i tots els serveis en producció.
- Els **dos centres de dades** i la infraestructura associada.
- Els equips d'**explotació, desenvolupament, sistemes i suport**.
- Els **proveïdors crítics** d'infraestructura, telecomunicacions i serveis.

3. Responsabilitats

La taula següent resumeix les responsabilitats respecte a aquesta política:

Rol	Responsabilitat respecte a aquesta política
Direcció	Aprovar la política i assignar els recursos necessaris per al seu compliment.
CISO	Mantenir la política actualitzada, coordinar la seva integració amb el SGSI i difondre-la.
Comitè de Seguretat	Supervisar el compliment de la política i avaluar l'activació dels plans de continuïtat.
Responsables d'Àrees Crítiques	Assegurar que els seus equips coneixen i apliquen la política en el seu àmbit.
Tots els empleats	Conèixer les seves funcions dins del BCP, participar en la formació i proves de continuïtat, i reportar incidents.

4. Comunicació i Disponibilitat

Aquesta política compleix amb els requisits de comunicació establerts en ISO 22301 (5.2.2):

Requisit	Com es compleix
a) Informació documentada	Política versionada amb control de canvis. Còpia signada a l'arxiu de seguretat.
b) Comunicada dins de l'organització	Sessions de formació i conscienciació. Canal Teams ENS-ISO. Base de coneixement accessible a tot el personal.
c) Disponible per a parts interessades	Publicada al web corporatiu de Smarting en tres idiomes (ES, CA, EN). Disponible sota petició per a clients i auditors.

5. Revisió

- Aquesta política es revisarà **anualment** com a part de la Revisió per la Direcció.
- Es revisarà **anticipadament** quan es produeixin:
  - Canvis significatius en els serveis, la infraestructura o l'estructura organitzativa.
  - Nous requisits legals, reguladors o contractuals.
  - Lliçons apreses d'incidents o exercicis que requereixin ajustos en els compromisos.
- La revisió es documentarà en les actes del Comitè de Seguretat i en el Registre de canvis (cont.3.3).

6. Relació amb la Política de Seguretat

Aquesta política complementa l'apartat 16 (Continuïtat de l'activitat) de la **Política de Seguretat de la Informació** (SGSI.PR.01.ca) de **Smarting**. Ambdues polítiques comparteixen l'estructura de govern del Comitè de Seguretat i es gestionen de forma integrada.

7. Aprovació

Mitjançant l'aprovació d'aquesta política, la Direcció de **Smarting Engineering, S.L.** manifesta la seva determinació i compromís en assolir un nivell de resiliència i continuïtat operativa adequat a les necessitats del negoci, garantint la protecció dels serveis crítics, la informació i les persones de forma integrada i coherent amb el SGSI.

Aprovat per:	Direcció de **Smarting Engineering, S.L.**
Data:	06/03/2026
Signatura:	La Direcció

Nota: Els documents esmentats en la present política són d'actualització periòdica i es troben disponibles per a la seva consulta per les parts interessades. Es poden sol·licitar a **security@smarting.es**