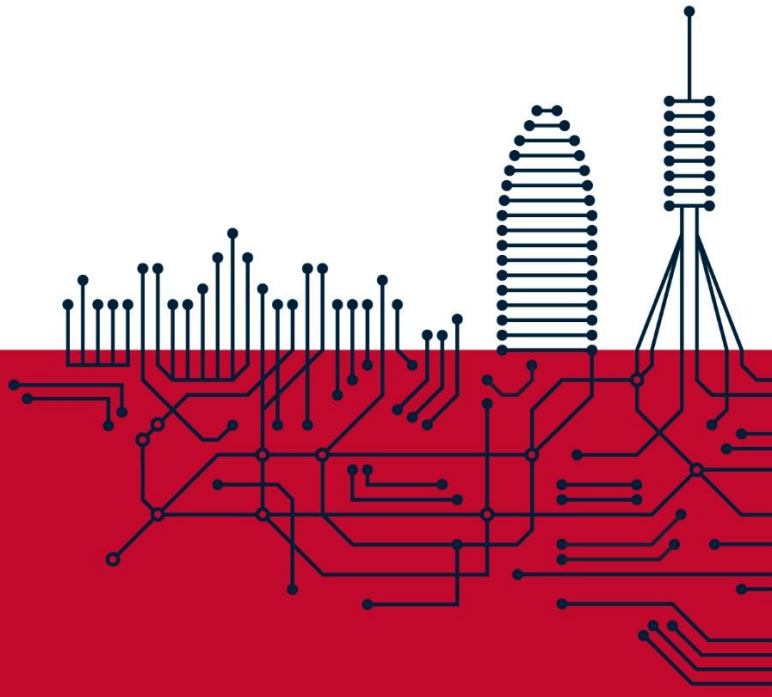
Smarting
ENGINEERING



Política
Seguretat de la Informació

SGSI.PR.01.ca v1.2

31/03/2026

1. Declaració de la Direcció

A **Smarting**, la confidencialitat, integritat i disponibilitat de la informació que tractem —pròpia, dels nostres clients i dels nostres usuaris— són elements estratègics per garantir la confiança, el compliment normatiu i la sostenibilitat del negoci.

La Direcció de **Smarting Engineering, S.L.** declara el seu compromís amb l'establiment, implementació, manteniment i millora contínua del **Sistema de Gestió de Seguretat de la Informació (SGSI)**, alineat amb els estàndards ISO/IEC 27001:2022, l'Esquema Nacional de Seguretat (ENS, RD 311/2022) en categoria MITJANA, i complementat pel Sistema de Gestió de Continuïtat del Negoci (SGCN) basat en ISO 22301:2019.

La Direcció assumeix els compromisos següents:

1.1. Apropiada al propòsit de l'organització

- **Smarting** desenvolupa solucions digitals i presta suport operatiu a clients i proveïdors, sent la plataforma Motorcloud i els serveis associats els actius essencials de l'organització.
- Protegir la **confidencialitat, integritat, disponibilitat, traçabilitat i autenticitat** de la informació manejada en el **desenvolupament de solucions**, la prestació de serveis i el **suport a clients institucionals**.
- Integrar la seguretat de la informació en tots els processos de negoci, des del disseny i desenvolupament fins a l'operació i el suport.
- Mantenir la confiança dels nostres clients, en particular de les **autoritats de transport i operadors** que confien en els nostres serveis.

1.2. Marc de referència per als objectius de seguretat

Aquesta política proporciona el marc per establir **objectius mesurables** de seguretat de la informació, alineats amb la direcció estratègica de l'organització. Els objectius es concreten anualment en la Revisió per la Direcció i compleixen el criteri SMART.

- **RTO** (Recovery Time Objective): temps objectiu de recuperació dels serveis crítics.
- **RPO** (Recovery Point Objective): pèrdua màxima de dades acceptable.
- Maduració operativa: **MTTD, MTTR, cobertura de backups 3-2-1**, consolidació del SIEM i EDR.
- Certificació normativa: manteniment d'ENS MITJANA i ISO 27001, certificació ISO 22301 i preparació cap a ENS Categoria Alta.

1.3. Compromís de complir els requisits aplicables

Complir amb tots els **requisits legals, reguladors, contractuals i normatius** aplicables a la seguretat de la informació, incloent-hi:

- **ISO/IEC 27001:2022** i els controls de l'Annex A.
- **ENS (RD 311/2022)** en categoria MITJANA, amb orientació cap a categoria Alta.
- **RGPD / LOPDGDD** en matèria de protecció de dades personals.
- **ISO 22301:2019** com a referència per a la continuïtat del negoci.
- **Directiva NIS2** com a referència per a la preparació de l'organització davant futures obligacions.

- **Requisits contractuals** amb clients, especialment amb l'Autoritat del Transport Metropolità de Barcelona (ATM).

Proporcionar els **recursos necessaris** (humans, tècnics, formatius i econòmics) per a l'establiment, implementació i millora contínua del SGSI.

1.4. Compromís de millora contínua del SGSI

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

- **Anàlisi i gestió de riscos** periòdica amb metodologia MAGERIT.
- **Auditories internes i externes** anuals (ENS, ISO 27001) i proves de seguretat (pentesting).
- **Revisió per la Direcció** anual conforme a la clàusula 9.3 de la norma.
- **Gestió de no conformitats i accions correctives** traçada en YouTrack.
- **Integració de lliçons apreses** d'incidents i simulacres.

Promoure una **cultura de seguretat** mitjançant formació periòdica i sensibilització de tot el personal, garantint l'adaptabilitat del SGSI als canvis tecnològics, organitzatius, reguladors i de l'entorn d'amenaces.

2. Abast

Aquesta política s'aplica a tots els **processos, recursos, tecnologies, infraestructures i persones** inclosos en l'abast del SGSI, així com a proveïdors i tercers que puguin impactar en la seguretat de la informació de Smarting. Això inclou:

- El **desenvolupament de solucions digitals** de Smarting, incloent la plataforma Motorcloud i els seus serveis.
- L'**operació dels serveis** prestats a clients i proveïdors.
- La **infraestructura tecnològica** associada (centres de dades, xarxes, sistemes i plataformes).
- Tot el **personal** de Smarting, amb independència del seu règim contractual o ubicació.
- Els **proveïdors i tercers crítics** que tracten informació de Smarting o dels seus clients.

3. Marc Organitzatiu de la Seguretat

Smarting ha identificat i definit els rols i funcions de seguretat necessaris per garantir la protecció de la informació, conforme al capítol II del **Reial Decret 311/2022** i la clàusula 5.3 d'ISO 27001:2022.

3.1. Comitè de Seguretat

Smarting ha constituït un **Comitè de Seguretat** que supervisa el compliment del SGSI i del SGCN. Les seves funcions són:

- Coordinar totes les activitats relacionades amb la seguretat de la informació i la continuïtat del negoci.
- Proposar i revisar la Política de Seguretat i la Política de Continuïtat.
- Aprovar les normes, procediments i requisits de formació en matèria de seguretat.
- Supervisar la gestió d'incidents, no conformitats i accions correctives.
- Avaluar l'activació dels plans de continuïtat davant disrupcions.

3.2. Rols principals

Els nomenaments de **CISO**, **Responsable del Servei (RE)** i **DPO** són aprovats per la Direcció a proposta del Comitè de Seguretat i es revisen cada dos anys o quan el lloc quedi vacant. La funció de Responsable de la Informació (**CIO**) recau en el **CTO**.

3.3. Resolució de conflictes

Smarting ha definit el procés i jerarquia per a la **resolució de conflictes d'autoritat** entre els perfils crítics amb responsabilitats en seguretat, aplicable a tots els perfils del SGSI i del SGCN.

4. Anàlisi i Gestió de Riscos

Tots els sistemes subjectes a aquesta política s'avaluen mitjançant una **anàlisi de riscos** basada en metodologia **MAGERIT**, valorant amenaces, vulnerabilitats i impactes. Aquesta anàlisi es repeteix:

- Regularment, almenys una vegada a l'any.
- Quan canviï la informació manejada.
- Quan canviïn els serveis prestats.
- Quan es produeixi un incident greu de seguretat.
- Quan es reportin vulnerabilitats greus.

5. Categorització dels Sistemes

Smarting classifica els seus sistemes conforme a l'Annex II de l'ENS en categories **Bàsica, Mitjana o Alta**, en funció del nivell més alt de les dimensions de seguretat valorades (confidencialitat, integritat, disponibilitat, traçabilitat i autenticitat).

El procés de categorització contempla la identificació de sistemes i actius crítics, l'avaluació del valor de la informació (incloent categories especials del RGPD), l'anàlisi de riscos, el compliment normatiu, la dependència entre sistemes, els requisits de les dimensions de seguretat i la capacitat de recuperació. Quan un client determini una categorització pròpia, **prevaldrà la categoria establerta pel client**.

6. Gestió del Personal i Professionalitat

Tots els membres de **Smarting** tenen l'**obligació de conèixer i complir** aquesta política i la Normativa de Seguretat. El Comitè de Seguretat és responsable d'aplicar les mesures necessàries perquè la informació arribi als afectats.

Tots els empleats reben **sessions de conscienciació** en matèria de seguretat almenys una vegada a l'any, complementades amb un programa de conscienciació contínua i formació específica per a noves incorporacions.

El personal dedicat a tasques de seguretat compta amb la **qualificació apropiada** i rep la formació específica necessària per garantir la seguretat de les tecnologies de la informació en totes les fases del cicle de vida.

Els mateixos requisits s'exigeixen als proveïdors que presten serveis relacionats amb la seguretat, mitjançant un procediment formal d'avaluació de proveïdors.

7. Autorització i Control dels Accessos

Els sistemes d'informació de **Smarting** disposen de mecanismes formals d'**autorització, autenticació i traçabilitat** que permeten concedir, denegar o revocar accessos quan és necessari. L'accés es limita al mínim estrictament necessari per al desenvolupament de les funcions de cada persona o sistema.

8. Protecció de les Instal·lacions

Les instal·lacions de **Smarting** estan protegides davant danys que puguin afectar els sistemes que alberguen i davant accessos de persones no autoritzades, conforme als procediments vigents de protecció d'instal·lacions i infraestructures.

9. Adquisició de Productes i Serveis de Seguretat

Tota nova adquisició de **producte o servei de seguretat** que pugui afectar el SGSI s'avalua prèviament des del punt de vista funcional i de requisits de seguretat. La validació inclou prova formal del producte i comprovació de compliment.

Els productes de seguretat es prioritzen conforme al **Catàleg CPSTIC (CCN-STIC 105)**. Quan no existeix alternativa CPSTIC adequada, s'aplica un procediment formal de justificació, validació i aprovació pel Comitè de Seguretat.

Tot servei contractat s'avalua abans de la seva posada en producció per assegurar el compliment dels requisits mínims de seguretat definits en aquesta política i en la Normativa de Seguretat.

10. Principi de Mínim Privilegi

El SGSI de **Smarting** aplica el **Principi del Mínim Privilegi**: a cada usuari, procés, aplicació o dispositiu se li atorguen únicament els permisos estrictament necessaris per desenvolupar les seves funcions legítimes.

Aquest principi redueix l'exposició a ciberatacs i preveu l'acumulació indeguda de privilegis, aplicant-se tant a usuaris humans com a aplicacions, sistemes o dispositius connectats que requereixen privilegis per realitzar tasques necessàries.

11. Integritat i Actualització del Sistema

Qualsevol **canvi físic o lògic** sobre els sistemes d'informació es realitza únicament després de la seva aprovació formal i seguint un procediment documentat.

Les actualitzacions, pegats i canvis en especificacions s'analitzen per evitar la degradació de la seguretat i es gestionen els riscos introduïts pels canvis.

12. Protecció de la Informació Emmagatzemada i en Trànsit

La informació ha d'estar protegida durant tot el seu **cicle de vida**, tant en emmagatzematge com en transmissió, en suport electrònic i físic. S'apliquen procediments específics per al maneig, etiquetatge, tractament i eliminació segura de la informació.

13. Prevenció davant Sistemes Interconnectats

Les connexions amb sistemes d'informació externs es realitzen amb mesures de **protecció perimetral, control d'accessos i registre d'activitat** per detectar anomalies. Les connexions segueixen les directrius de les guies **CCN-STIC** publicades a aquest efecte.

14. Registre d'Activitat i Detecció de Codi Maliciós

Smarting supervisa els seus sistemes d'informació mitjançant **SIEM i eines EDR**, registrant esdeveniments rellevants com a incidències de seguretat. La supervisió respecta els requisits legals de privacitat i s'utilitza per verificar l'eficàcia dels controls i el compliment de la política de control d'accessos.

Tots els equips corporatius disposen d'**eines antivirus d'última generació (EDR)** amb gestió centralitzada per a la protecció, detecció, recuperació i eliminació de codi maliciós.

La gestió d'incidents es traça en **YouTrack** conforme a la taxonomia **CCN-STIC 817**, amb notificació a les autoritats competents (CCN-CERT, AEPD, INCIBE) quan correspongui.

15. Gestió d'Incidents de Seguretat

La Direcció de **Smarting** ha establert un **procediment formal de notificació** d'incidents de seguretat. Tot el personal ha de notificar incidències mitjançant el canal habilitat (**security@smarting.es**) de forma immediata. Això garanteix una resposta ràpida i efectiva davant incidències i debilitats.

16. Continuïtat de l'Activitat

Smarting disposa d'un **Sistema de Gestió de Continuïtat del Negoci (SGCN)** basat en **ISO 22301:2019** que complementa el SGSI. El SGCN garanteix la capacitat de l'organització per mantenir els serveis essencials i recuperar-se davant disrupcions, mitjançant:

- Una **Anàlisi d'Impacte en el Negoci (BIA)** que identifica processos crítics i temps de recuperació.
- Un **Pla de Continuïtat del Negoci (BCP)** que coordina la resposta operativa.
- **Plans Tecnològics de Recuperació (DRP)** que cobreixen la restauració de la infraestructura.
- **Proves periòdiques i simulacres** que validen l'eficàcia dels plans.

La gestió de la continuïtat es regeix per la seva política específica, definida a la **Política de Continuïtat del Negoci** (SGCN.PR.01.ca), que complementa el present apartat.

17. Millora Contínua del SGSI

La Direcció es compromet a **desenvolupar, implantar, mantenir i millorar contínuament** la present Política i el seu Sistema de Gestió, valorant especialment la confidencialitat, integritat, disponibilitat, traçabilitat i autenticitat de la informació crítica.

La millora contínua s'articula mitjançant **auditories, revisions per la direcció, anàlisi d'indicadors, gestió de no conformitats** i la integració de lliçons apreses d'incidents i exercicis.

18. Dades de Caràcter Personal

Smarting tracta dades de caràcter personal complint el **RGPD** i la **LOPDGDD**. Considerant l'estat de la tècnica, els costos, la naturalesa i els riscos del tractament, **Smarting** ha aplicat mesures tècniques i organitzatives apropiades, entre d'altres:

- Seudonimització i xifratge de dades personals.
- Capacitat de garantir la confidencialitat, integritat, disponibilitat i resiliència permanents dels sistemes de tractament.
- Capacitat de restaurar la disponibilitat i l'accés a les dades personals ràpidament en cas d'incident físic o tècnic.
- Processos de verificació, avaluació i valoració regulars de l'eficàcia de les mesures.

La supervisió del tractament de dades personals recau en la figura del **DPO**, designat conforme al RGPD.

19. Estructuració de la Documentació de Seguretat

La documentació de seguretat segueix les directrius establertes en els procediments de control documental, amb mesures per estructurar, gestionar i controlar l'accés a la documentació, garantint la seva integritat i confidencialitat.

La documentació es gestiona a la **Base de Coneixement corporativa**, amb control de versions, traçabilitat de canvis i accés restringit a personal autoritzat: membres del Comitè de Seguretat, representants del client i consultors o auditors autoritzats.

20. Documentació i Comunicació

Aquesta política compleix amb els requisits de comunicació establerts en ISO 27001 (5.2):

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.

21. Revisió i Actualització

Aquesta política es revisa **anualment** com a part de la Revisió per la Direcció. Es revisa **anticipadament** quan es produeixen:

- 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.
- Canvis significatius en l'entorn d'amenaces o en el context del negoci.

La revisió es documenta a les actes del Comitè de Seguretat i a la Revisió per la Direcció.

22. 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 seguretat adequat a les necessitats del negoci, garantint la protecció de la informació, els serveis i les persones de forma integrada i coherent amb el SGCN.

Aprovat per:	Direcció de **Smarting Engineering, S.L.**
Data:	31/03/2026
Signatura:	Jordi Tirado (CEO) Dani Fernández (CTO)

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**