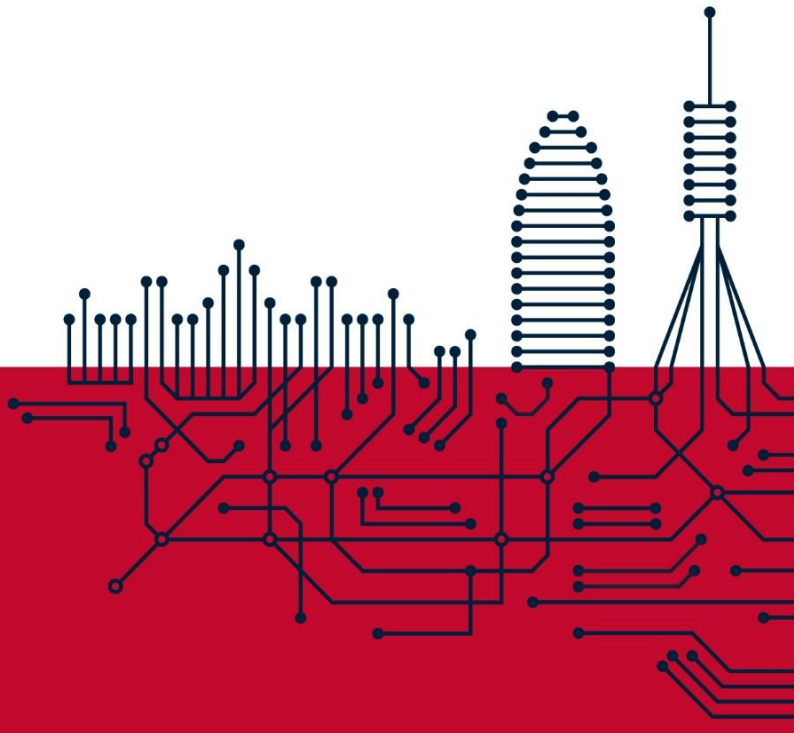
Smarting
ENGINEERING

Política de Seguretat de la Informació



SGSI.PR.01.es

Versió	1.0
Data	12/02/2024

> Go beyond

CONTINGUT

1. OBJECTIUS I MISSIÓ DE SMARTING

Smarting, com a empresa especialitzada en el desenvolupament de solucions digitals de ticketing per al transport públic, reconeix la importància crítica de la seguretat de la informació en l' èxit continu de les seves operacions i la satisfacció de les seves parts interessades. Aquesta política estableix el marc per gestionar la seguretat de la informació en l'organització d'acord amb els principis i requisits de la norma ISO 27001 i de l'ENS (Esquema Nacional de Seguretat).

Objectius de Seguretat de la Informació

La política de seguretat de la informació de **Smarting** té com a objectius fonamentals:

- Garantir la confidencialitat, integritat i disponibilitat de la informació crítica de l' empresa i dels seus clients, així com assegurar la traçabilitat i autenticitat.
- Complir amb les lleis, regulacions i requisits contractuals aplicables a la seguretat de la informació en l' àmbit del transport públic
- Fomentar una cultura de consciència i responsabilitat en la gestió de la seguretat de la informació entre els empleats.
- Establir i mantenir un sistema de gestió de la seguretat de la informació que promogui la millora contínua i l' adaptabilitat als canvis tecnològics i empresarials.

Compromís amb la Seguretat de la Informació

L' alta direcció de **Smarting**, representada pel CEO i el CTO, es compromet a:

- Proporcionar recursos adequats per implementar i mantenir un sistema de gestió de la seguretat de la informació efectiu.
- Establir rols i responsabilitats clars per a la gestió de la seguretat de la informació en tots els nivells de l' organització.
- Fomentar la participació dels empleats en la protecció de la informació i proporcionar la formació necessària per millorar les competències en seguretat de la informació.
- Avaluar periòdicament l' acompliment del sistema de gestió de la seguretat de la informació i realitzar ajustaments segons sigui necessari.

2. MARC LEGAL I REGULATORI

Smarting durà a terme les seves activitats d' acord amb el marc legal i regulatori vigent. Es compromet a complir amb totes les lleis i regulacions pertinents relacionades amb la seguretat de la informació, incloent-hi, però no limitant-se a les indicades en el document SGSI.RG.01.es, en el full Marc Legal.

Smarting integra l' ENS i la ISO 27001 en la política de seguretat de l' organització per brindar una estructura més completa i robusta per abordar els aspectes específics de la seguretat de la informació, tant a nivell nacional com internacional. A més, l' adopció d' aquests estàndards millora la credibilitat de l' empresa, demostrant el seu compromís amb les millors pràctiques de seguretat.

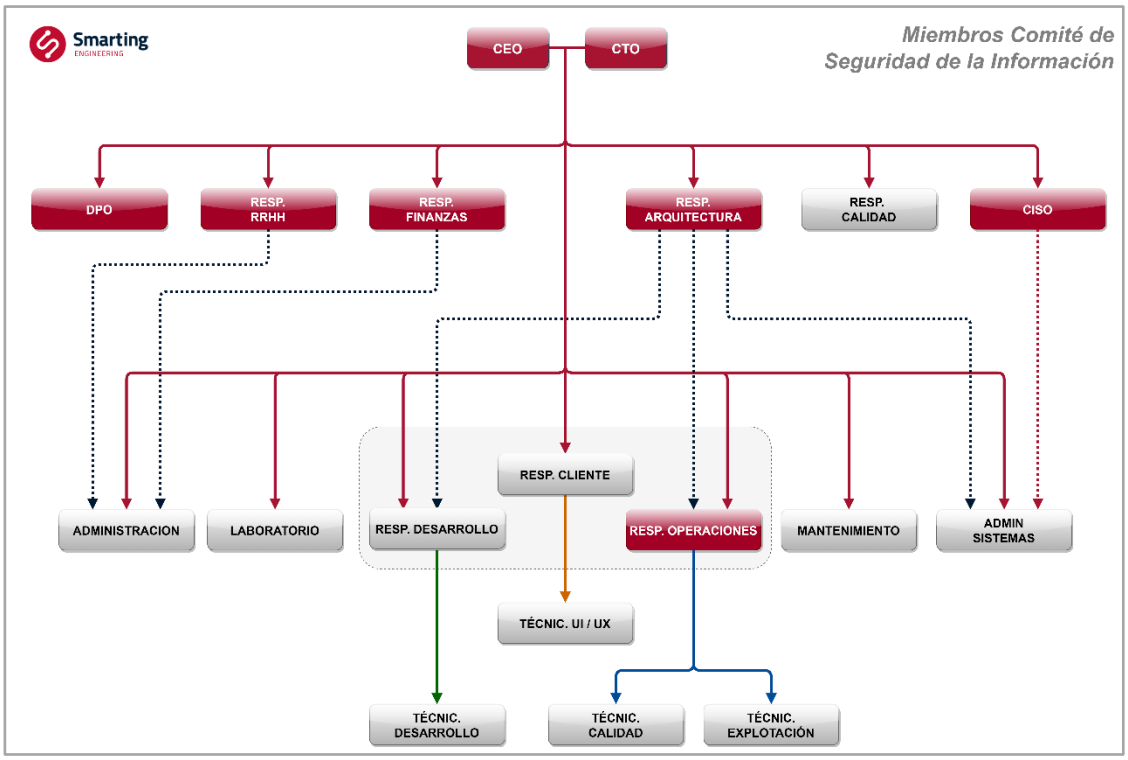
3. MARC ORGANITZATIU DE LA SEGURETAT

La present política de seguretat ha establert d'acord amb els principis bàsics assenyalats en el capítol II del Reial decret 311/2022 i s'ha desenvolupat aplicant els següents requisits mínims:

Smarting **ha identificat i definit els rols i funcions de seguretat necessaris** per garantir la protecció de la informació. Cada rol té responsabilitats clarament definides (SGSI.RG.04.es - Persones).

Smarting **ha nomenat un Comitè de Seguretat** (SGSI.DC.00.es – Acta designació Comitè) que supervisarà el seguiment i compliment del SGSI. El Comitè de Seguretat està format per càrrecs corporatius i de responsabilitat dins de l'organització La relació dels membres constituents del Comitè de Seguretat queda definit en el registre creat a l'efecte (SGSI.RG.04.es - Persones). Aquest comitè de Seguretat TIC tindrà les següents funcions i responsabilitats:

- Coordinar totes les activitats relacionades amb la seguretat de les TIC.
- És responsable de la redacció de la Política de Seguretat.
- És responsable de la creació i aprovació de les normes que emmarquen l' ús dels serveis TIC.
- Aprovarà els procediments d' actuació pel que fa a l' ús dels serveis TIC.
- Aprovarà els requisits de formació i qualificació d' administradors, operadors i usuaris des del punt de vista de seguretat de les TIC.

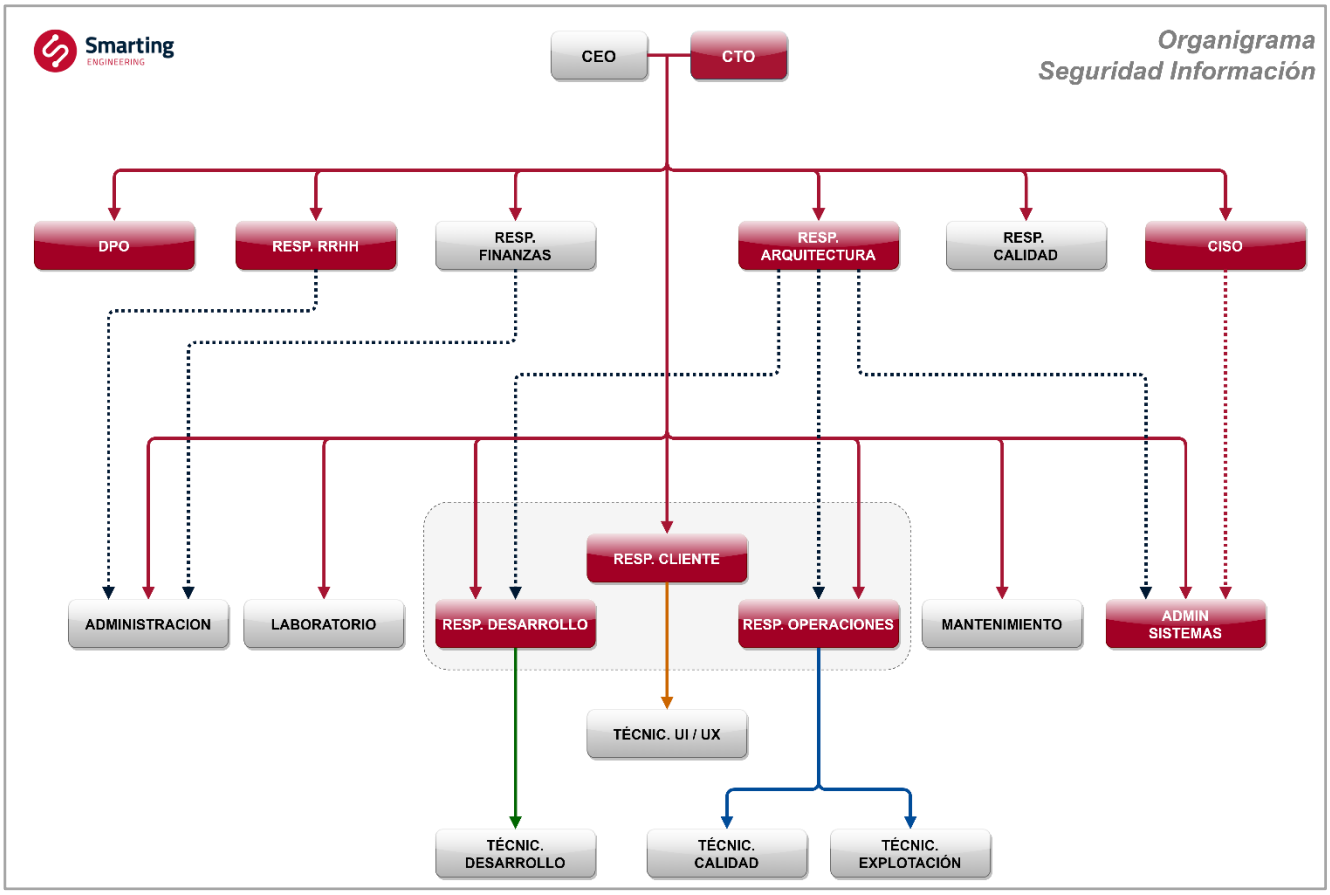


Així mateix, s'han definit les funcions i responsabilitats del responsable de Seguretat, del responsable de la Informació i del responsable dels Serveis, així com la relació d'aquests amb el Comitè de Seguretat (SGSI.RG.04.es - Persones).

Per tal de descriure el procés i jerarquia per resoldre conflictes d'autoritat que pugui ocórrer durant la gestió de l'ENS entre els perfils crítics amb responsabilitats en matèria de seguretat, a Smarting **s'ha definit les funcions per a la resolució de conflictes davant responsables** i que aplica a tots els perfils específics de gestió de l'ENS (SGSI.RG.04.es - Persones).

El responsable de Seguretat de la Informació (CISO), el responsable del Servei (RE) i el responsable de Protecció de Dades (DPO) seran nomenats per la Direcció a proposta del Comitè de Seguretat. Aquests nomenaments es revisaran cada 2 anys o quan el lloc quedi vacant. El responsable de la Informació (CIO) recau en Smarting en la figura del responsable Tecnològic (CTO)

En el següent organigrama es marquen els llocs amb funcions o responsabilitats relacionades amb la seguretat de la informació. L' escalació en absència d' algun d' aquests responsables es realitzarà segons les línies jeràrquiques marcades en aquest diagrama.



4. ANÀLISI I GESTIÓ DE RISCOS

Tots els sistemes subjectes a aquesta Política han estat avaluats mitjançant una anàlisi de riscos, avaluant les amenaces i els riscos als quals estan exposats. Aquesta anàlisi es repetirà:

- regularment, almenys una vegada a l' any
- quan canviï la informació manejada
- quan canviïn els serveis prestats
- quan s' esdevingui un incident greu de seguretat
- quan es reportin vulnerabilitats greus

5. CATEGORITZACIÓ DELS SISTEMES

Smarting ha definit els criteris per determinar el nivell de seguretat requerit en cada sistema d'informació. Per a això s' analitzen els elements essencials, informació i serveis, pivotant al voltant d' ells els criteris que el responsable de cada tipus d' informació i cada servei podrà utilitzar, considerant que la facultat de determinar la categoria del sistema correspon al responsable d' aquest.

L'Esquema Nacional de Seguretat estableix en el seu Annex II mesures de seguretat condicionades a la valoració del nivell de seguretat en cada dimensió i a la categoria de seguretat (article 40) del sistema d'informació respectiu. Al seu torn, la categoria de seguretat del sistema es calcula en funció del nivell de seguretat més alt de les dimensions valorades.

La categorització dels sistemes d'informació en Bàsica, Mitjana o Alta segons els criteris de l'Esquema Nacional de Seguretat (ENS) implica avaluar diversos factors que afecten la seguretat de la informació. A continuació, es descriu el procés general per determinar la categorització dels sistemes d' informació de **Smarting**.

- **Identificació dels Sistemes d' Informació:**
  - Enumerar i classificar tots els sistemes d' informació que maneja l' organització.
- **Avaluació del Valor de la Informació:**
  - Analitzar la importància i el valor de la informació manejada per cada sistema.
  - Considerar la confidencialitat, integritat i disponibilitat de les dades.
  - Es consideren **dades personals sensibles**:
    - Dades relatives a la salut.
    - Dades genètiques i biomètriques.
    - Dades relatives a la sexualitat o orientació sexual.
    - Dades personals que revelin l' origen racial o ètnic, les opinions polítiques i les conviccions religioses o filosòfiques.
    - Dades sobre l' afiliació sindical.
  - Es classifica la informació pel **seu nivell de confidencialitat:** **SGSI.PR.06.es – 4.1.1. Nivells de classificació**
  - Es classifica la informació pel seu **impacte:** **SGSI.PR.06.es – 4.1.2. Classificació de la informació**
- **Identificació d' Actius Crítics:**
  - Identificar els actius crítics per al funcionament i la continuïtat del negoci.
  - Determinar com la pèrdua o compromís d' aquests actius afectaria l' organització.
- **Anàlisi de Riscos:**
  - Realitzar una avaluació de riscos per a cada sistema.
  - Identificar amenaces, vulnerabilitats i possibles impactes en la seguretat de la informació.
- **Compliment Normatiu:**
  - Avaluar el compliment dels sistemes amb els requisits legals i normatius, incloent aquells establerts a l' ENS.
- **Nivell d' Exposició:**
  - Determinar el nivell d' exposició a riscos de seguretat per a cada sistema.
  - Avaluar la probabilitat i gravetat de possibles incidents de seguretat.
- **Dependència d' altres Sistemes:**
  - Considerar la interconnexió i dependència entre diferents sistemes d' informació.
  - Avaluar com l' afectació d' un sistema podria tenir repercussions en d' altres.
- **Requisits de Confidencialitat, Integritat i Disponibilitat:**
  - Avaluar els requisits específics de confidencialitat, integritat i disponibilitat per a cada sistema.
  - Comparar aquests requisits amb els nivells establerts a l' ENS.
- **Avaluació de Capacitat de Recuperació:**

- Avaluar la capacitat de recuperació de cada sistema davant de possibles incidents de seguretat.
- Considerar l' existència de plans de continuïtat del negoci i mesures de recuperació.

- **Definició de Categoria**:
  - Classificar cada sistema en una de les categories establertes per l'ENS **(Bàsica, Mitjana, Alta)** segons els resultats de l'avaluació.
  - Quan un client determini una categorització per als sistemes d' informació que Smarting li ofereix, **prevaldrà la categoria establerta pel Client**.
- **Documentació i Revisió Contínua:**
  - Documentar la categorització de cada sistema d' informació.
  - Revisar periòdicament la categorització per assegurar-se que continuï sent adequada i ajustar-la segons sigui necessari.

6. GESTIÓ DEL PERSONAL I PROFESSIONALITAT

Tots els membres de Smarting tenen l' obligació de conèixer i complir aquesta Política de Seguretat de la Informació i la Normativa de Seguretat, essent responsabilitat del Comitè de Seguretat aplicar les mesures necessàries perquè la informació arribi als afectats.

Tots els empleats rebran una sessió de conscienciació en matèria de seguretat almenys una vegada a l' any. Així mateix, s' establirà un programa de conscienciació contínua per sensibilitzar tots els membres de Smarting, en particular als de nova incorporació, el qual es troba alineat amb altres estàndards implementats.

El personal que estigui dedicat a les tasques de seguretat està qualificat de manera apropiada, atesa la sensibilitat i complexitat d' algunes d' aquestes tasques. Això és aplicable a totes les fases del cicle de vida del procés de seguretat (instal·lació, manteniment, gestió d'incidències i desmantellament). Per a això el personal rep la formació específica necessària per garantir la seguretat de les tecnologies de la informació aplicables als sistemes i serveis subjectes a l' ENS.

Lògicament, els mateixos requisits requerits internament s' han d' exigir a qualsevol proveïdor que presti serveis relacionats amb seguretat. Per a això des de Smarting s'ha impulsat un procediment per a l'avaluació dels proveïdors de manera que s'asseguri el nivell de seguretat similar al requerit per l'entitat.

7. AUTORITZACIÓ I CONTROL DELS ACCESSOS

El primer pas per assegurar que la informació i els sistemes estan protegits és limitar-ne l'accés. Per això, s' ha definit els qui, i en quina mesura tindran accés als recursos, de manera que cadascú tingui l' accés necessari per realitzar les seves tasques, però no a equips o dades que no han d' estar al seu abast.

Així mateix, els sistemes d'informació de Smarting compten amb mecanismes d'autorització per permetre l'accés i denegar-lo i revocar-lo quan sigui necessari.

8. PROTECCIÓ DE LES INSTAL·LACIONS

Les instal·lacions es troben protegides contra danys que puguin afectar els sistemes que alberguen i contra accessos de persones no autoritzades. L'accés a les nostres instal·lacions està securitzat i es troba regulat en el procediment habilitat a aquest efecte (SGSI.PR.03.es - Procediments).

9. ADQUISICIÓ DE PRODUCTES DE SEGURETAT I CONTRACTACIÓ DE SERVEIS DE SEGURETAT.

Smarting estableix els requisits del negoci i de seguretat de la informació per als seus sistemes d'informació, ja siguin nous o bé existents i que s'amplïin o millorin.

Així, tota nova adquisició de producte i serveis de seguretat que pugui afectar el SGSI s' haurà d' avaluar prèviament, des del punt de vista funcional i de requisits de seguretat necessaris. Després de la validació, es procedirà amb la prova formal del producte indicant si compleix amb els requisits.

Tot servei contractat haurà de ser avaluat abans de la seva posada en producció per tal d' assegurar que compleixi amb els requisits mínims de seguretat definits en la present Política de Seguretat de la Informació i la Normativa de Seguretat vigent.

10. MÍNIM PRIVILEGI

El Sistema de Seguretat de la Informació implementat en **Smarting** segueix el Principi del Mínim Privilegi segons el qual s'atorga als usuaris del sistema els nivells (o permisos) d'accés mínims necessaris per desenvolupar les seves funcions, amb l'objectiu de restringir l'accés a la informació i recursos únicament al que és estrictament necessari per complir amb una tasca específica.

Aquest principi de mínim privilegi garanteix que cada part (ja sigui un procés, un usuari o un programa) només pugui accedir al que és essencial per al seu propòsit legítim, no atorgant privilegis innecessaris. No obstant això, aquest principi no es limita només a l' accés dels usuaris humans també s' aplica a aplicacions, sistemes o dispositius connectats que requereixen privilegis per realitzar tasques necessàries.

En limitar els privilegis es redueix l'exposició a ciberatacs i s'evita l'acumulació de privilegis.

11. INTEGRITAT I ACTUALITZACIÓ DEL SISTEMA

Per garantir la integritat dels sistemes d' informació sempre, qualsevol canvi físic i lògic, es realitza només després de la seva aprovació formal i mitjançant un procediment formal.

Per a això, s' actualitzen els sistemes de manera controlada i segons l' estat de seguretat requerit en cada moment. Els canvis en les especificacions dels fabricants, l' aparició de noves vulnerabilitats, l' emissió d' actualitzacions i pegats que afectin els sistemes són analitzats per prendre les mesures necessàries perquè no es degradin els sistemes ni el seu nivell de seguretat, gestionant així mateix els riscos que introdueixen els canvis que es realitzaran.

12. PROTECCIÓ DE LA INFORMACIÓ EMMAGATZEMADA I EN TRÀNSIT

Una part significativa del cicle de vida de la informació correspon al seu emmagatzematge i al seu transport. La informació ha d' estar protegida en tot moment. Per a això s' han desenvolupat procediments adequats, que cobreixen tant a la informació en suport electrònic com en paper, així com política per al maneig i el tractament de la informació.

13. PREVENCIÓ DAVANT D' ALTRES SISTEMES D' INFORMACIÓ INTERCONNECTATS.

La prevenció davant d'altres sistemes d'informació interconnectats és un aspecte crucial per a **Smarting**. Per a això s' han establert mesures per garantir la seguretat quan els sistemes d' informació es connecten entre si, tenint en compte, aspectes tals com la protecció del perímetre, el control d' accessos o el degut registre d' activitat amb el qual poder detectar possibles anomalies o comportaments inusuals en la interconnexió.

Qualsevol connexió feia o des de serveis interconnectats seran realitzats seguint les directrius definides a les guies CCN-STIC publicades a l' efecte.

14. REGISTRE DE L' ACTIVITAT I DETECCIÓ DE CODI DANYÓS.

L' empresa realitza la supervisió dels seus sistemes d' informació i processament registrant-les com a incidències de seguretat, revisant el registre d' operació i fallades dels seus sistemes per identificar el problema. Així, les activitats de supervisió de l'ús dels sistemes de **Smarting** respecten els requisits legals de privacitat i s'utilitzen per verificar l'efectivitat dels controls de seguretat implantats i el compliment de la política de control d'accessos.

Així mateix, els equips corporatius, mitjançant l'ús d'antivirus d'última generació (EDR) amb gestió centralitat, compten amb eines per a la protecció, detecció, recuperació i eliminació de codi maliciós.

15. INCIDENTS DE SEGURETAT

Des de la direcció de **Smarting** s'ha establert un procediment de notificació formal pel qual tot el personal ha de notificar incidències relacionades amb la seguretat mitjançant el canal establert (security@smarting.es) de forma immediata i sense demores. Això permet garantir una resposta ràpida i efectiva davant incidències i debilitats en la seguretat.

16. CONTINUÏTAT DE L' ACTIVITAT

L' empresa ha establert un procediment per actuar contra interrupcions en l' activitat empresarial i protegir els processos crítics dels efectes de fallades importants en els sistemes d' informació i assegurar el seu restabliment immediat. Per això, s'ha implementat un pla de continuïtat de negoci (**SGSI.RG.03.es | Valoració BIA**) per reduir l'impacte sobre la infraestructura de **Smarting**, i conseqüentment sobre l'empresa, i la recuperació d'actius d'informació (ja sigui per accidents, fallada en equipament, actes deliberats, etc.) de tal manera que els processos del departament assoleixin un nivell acceptable de continuïtat mitjançant mesures de recuperació correctives i preventives.

17. MILLORA CONTÍNUA DEL PROCÉS DE SEGURETAT

La Direcció, per la seva banda, valora especialment i estableix com a criteri principal per a l' estimació dels seus riscos, la valoració de la confidencialitat, integritat i disponibilitat de la informació crítica de l' empresa i dels seus clients, així com assegurar la traçabilitat i autenticitat d' aquests.

Així, es compromet a desenvolupar, implantar, mantenir i millorar contínuament la present **Política de Seguretat** i el seu **Sistema de Gestió** amb l' objectiu de la millora contínua en la forma en què presten els seus serveis i en què tracten la informació.

18. DADES DE CARÀCTER PERSONAL

Smarting tracta dades de caràcter personal. En aquest sentit, i en compliment amb la legislació vigent en matèria de protecció de dades, tenint en compte l' estat de la tècnica, els costos d' aplicació, i la naturalesa, l' abast, el context i les finalitats del tractament, així com riscos de probabilitat i gravetat variables per als drets i llibertats de les persones físiques, **Smarting** ha aplicat mesures tècniques i organitzatives apropiades per garantir un nivell de seguretat adequat al risc, que en el seu cas inclogui, entre d' altres:

- la pseudonimització i el xifrat de dades personals;
- la capacitat de garantir la confidencialitat, integritat, disponibilitat i resiliència permanents dels sistemes i serveis de tractament;
- la capacitat de restaurar la disponibilitat i l'accés a les dades personals de forma ràpida en cas d'incident físic o tècnic;
- un procés de verificació, avaluació i valoració regulars de l' eficàcia de les mesures tècniques i organitzatives per garantir la seguretat del tractament.

19. ESTRUCTURACIÓ DE LA DOCUMENTACIÓ DE SEGURETAT

La documentació de seguretat del sistema seguirà les directrius establertes per **Smarting**. S' implementaran mesures per estructurar, gestionar i controlar l' accés a la documentació de seguretat, garantint la seva integritat i confidencialitat. L' accés estarà restringit a personal autoritzat i es durà a terme d' acord amb les polítiques d' accés definides.

S' ha creat un canal específic **ENS-ISO27001** en Microsoft Teams, dins de l' equip general de normes ISO creat per a la gestió de Normes. S' assignaran els permisos necessaris a les persones que poden tenir accés a aquesta documentació: Membres del Comitè de Seguretat de la Informació, Representants del Client i Consultors i Auditors de Seguretat de la Informació.

La documentació es repartirà en carpetes distingint entre ISO i ENS. L'estructura de carpetes interna seguirà, quan es consideri oportú per facilitar la seva classificació, els apartats de les respectives normes/reglamentacions.

La documentació generada per al Sistema de Gestió de Seguretat de la Informació de **Smarting** seguirà l'estructura d'identificació definida en **SGSI.RG.01.es - Sistema**. En aquest document es porta també el registre de documentació i el control de versions.

20. DOCUMENTACIÓ I COMUNICACIÓ

Aquesta Política de seguretat de la Informació estarà disponible com a informació documentada i es comunicarà dins de l' organització. A més, es compartirà amb les parts interessades rellevants, com autoritats, operadors i usuaris de transport públic, segons sigui apropiat.

21. REVISIÓ I ACTUALITZACIÓ

Aquesta política serà revisada anualment o abans si hi ha canvis significatius en l' entorn operatiu o tecnològic de **Smarting**. L' alta direcció es compromet a mantenir aquesta política alineada amb els objectius de l' empresa i els requisits de seguretat de la informació aplicables.

22. SIGNATURA DE LA DIRECCIÓ

Mitjançant l' aprovació d' aquesta política, la Direcció de Smarting manifesta la seva determinació i compromís a assolir un nivell de seguretat adequat a les necessitats del negoci que garanteixi la protecció dels actius de forma homogènia.

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