POLÍTICA DE SEGURETAT DE LA INFORMACIÓ

Índex

1. Aprovació i entrada en vigor

La present Política de Seguretat de la Informació ha estat aprovada per les Direccions de les entitats incloses en l'abast del Sistema de Gestió de Seguretat de la Informació (SGSI), d'acord amb l'Esquema Nacional de Seguretat (ENS) i amb la norma ISO/IEC 27001:2022

- Fundació Catalana de l'Esplai / Fundesplai.
- 7 i Tria, S.L.
- Fundación Esplai Ciudadanía Comprometida.

Aquesta Política serà vigent des de la data d'aprovació i romandrà en vigor fins que sigui substituïda per una nova versió.

2. Introducció

Les entitats incloses depenen dels sistemes d'informació per desenvolupar les seves activitats, prestar els seus serveis i complir els seus objectius. Aquests sistemes han de ser administrats amb diligència, aplicant mesures adequades i proporcionades al risc per protegir-los davant de danys accidentals o deliberats que puguin afectar la confidencialitat, la integritat, la disponibilitat, l'autenticitat i la traçabilitat de la informació tractada i dels serveis prestats.

L'objectiu últim de la seguretat de la informació és garantir que les entitats puguin desenvolupar les seves funcions i prestar els seus serveis amb qualitat, continuïtat i confiança, actuant preventivament, supervisant l'activitat i reaccionant amb rapidesa davant els incidents.

Els sistemes TIC (Tecnologies de la Informació i la Comunicació) han d'estar protegits davant amenaces canviants amb potencial impacte sobre la informació, els serveis, les persones usuàries, les entitats col·laboradores, els proveïdors i el funcionament intern. Per això, s'aplicarà una estratègia de seguretat basada en l'Esquema Nacional de Seguretat, en la norma ISO/IEC 27001:2022, en la gestió de riscos, en la vigilància contínua, en la resposta davant incidents i en la millora contínua.

La seguretat ha d'estar integrada en totes les fases del cicle de vida dels sistemes: concepció, adquisició, desenvolupament, implantació, explotació, manteniment i retirada. Els requisits de seguretat i les necessitats associades s'han de tenir en compte en la planificació, contractació, adquisició de serveis TIC, desenvolupament d'aplicacions, gestió de proveïdors i prestació de serveis.

3. Abast

Aquesta Política s'aplica als sistemes d'informació inclosos en l'abast ENS i en l'abast del SGSI de les entitats següents:

- Fundació Catalana de l'Esplai / Fundesplai.
- 7 i Tria, S.L.
- Fundación Esplai Ciudadanía Comprometida.

Les entitats incloses desenvolupen activitats educatives, socials, ambientals, de lleure educatiu, serveis escolars, formació, inclusió digital, acompanyament a entitats, projectes europeus, suport al Tercer Sector i gestió de serveis adreçats a persones, famílies, centres educatius, entitats socials, administracions i la comunitat en general.

La certificació es planteja de forma individual per a cada entitat. No obstant això, existeix un model tecnològic i de seguretat amb elements comuns i centralitzats, especialment pel que fa a infraestructura, plataformes corporatives, gestió tècnica, suport, control d'accessos, còpies de seguretat, seguretat tècnica, proveïdors i evidències.

La Política s'aplicarà a tot el personal, persones col·laboradores, tercers, proveïdors i prestadors de serveis que accedeixin a informació, actius o sistemes inclosos dins l'abast ENS i/o del SGSI (Sistema de Gestió de Seguretat de la Informació) de qualsevol de les entitats indicades.

4. Missió

Per assolir els seus objectius, les entitats assumeixen el seu compromís amb la seguretat de la informació, comprometent-se a la gestió adequada d'aquesta, amb la finalitat d'oferir a tots els seus clients les màximes garanties pel que fa a la seguretat de la informació utilitzada. Els sistemes seran administrats amb diligència, adoptant les mesures adequades per protegir-los davant danys accidentals o deliberats que puguin afectar la disponibilitat, la integritat o la confidencialitat de la informació tractada o dels serveis prestats.

En aquest sentit, la missió i els objectius de seguretat que aquesta Política pretén garantir són:

- Assegurar la confidencialitat, integritat, disponibilitat, autenticitat i traçabilitat de la informació.
- Garantir la continuïtat dels serveis inclosos en l'abast ENS i/o del SGSI.
- Implantar mesures de seguretat en funció del risc, de la categorització del sistema i dels requisits aplicables de l'ENS i/o del SGSI.
- Aplicar el principi de mínim privilegi i reforçar el deure de confidencialitat.
- Formar i conscienciar el personal en seguretat de la informació.
- Protegir els actius físics i lògics mitjançant controls proporcionals al risc.
- Establir controls de seguretat en les comunicacions, accessos remots, xarxes i serveis al núvol.
- Integrar la seguretat en l'adquisició, desenvolupament, manteniment i retirada de sistemes.
- Gestionar incidents per a la seva detecció, contenció, mitigació, resolució i prevenció de recurrències.
- Protegir les dades personals d'acord amb el RGPD (Reglament General de Protecció de Dades), la LOPDGDD (Llei Orgànica de Protecció de Dades Personals i Garantia dels Drets Digitals) i els riscos associats als tractaments.
- Supervisar de forma continuada l'estat de la seguretat i impulsar la millora contínua.

Els objectius de seguretat de la informació s'establiran, revisaran i actualitzaran periòdicament, de manera coherent amb aquesta Política, amb els riscos identificats, amb els requisits ENS i amb els requisits del SGSI d'acord amb la norma ISO/IEC 27001:2022.

5. Principis rectors de la política

La seguretat de la informació es regirà pels principis següents:

- **Abast estratègic**: la seguretat ha d'estar alineada amb la missió, els objectius i les activitats de les entitats incloses.
- **Seguretat integral**: la protecció ha de contemplar les persones, els processos, la informació, les instal·lacions, la tecnologia i els proveïdors.
- **Gestió basada en riscos**: les mesures de seguretat s'adoptaran en funció d'una anàlisi prèvia de riscos i seran proporcionals als riscos identificats.
- **Prevenció, detecció, resposta i recuperació**: s'impulsaran mesures per prevenir incidents, detectar-los a temps, respondre-hi adequadament i recuperar l'operativa afectada.
- **Defensa en profunditat**: s'establiran controls en diferents capes organitzatives, físiques, lògiques i operatives.
- **Vigilància i millora contínues**: l'estat de la seguretat es revisarà periòdicament per detectar desviacions i millorar els controls implantats.
- **Diferenciació de responsabilitats**: les funcions i responsabilitats en matèria de seguretat estaran definides de manera clara i separada, sempre que sigui possible.
- **Coordinació entre entitats**: els elements comuns del model tecnològic i de seguretat s'hauran de gestionar de manera coordinada entre les entitats incloses.

6. Marc normatiu

La present Política es fonamenta, entre d'altres, en les normes i referències següents:

- Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat.
- Reglament general de protecció de dades —RGPD, Reglament (UE) 2016/679.
- Llei orgànica 3/2018, de protecció de dades personals i garantia dels drets digitals —LOPDGDD—.
- Llei 9/2017, de contractes del sector públic, quan sigui aplicable.
- Llei 34/2002, de serveis de la societat de la informació i de comerç electrònic —LSSI-CE—.
- Guies CCN-STIC relacionades amb l'ENS.
- Norma ISO/IEC 27001:2022, Sistemes de Gestió de la Seguretat de la Informació.
- Normativa sectorial, contractual o administrativa aplicable als serveis prestats.

La identificació, revisió i seguiment dels canvis normatius i dels requisits legals aplicables es duu a terme d'acord amb el procediment **Determinació de les obligacions legals**. Per als requisits ambientals, de seguretat industrial i de pública concurrència, s'aplica addicionalment el procediment **Determinació de les obligacions legals, ambientals, de seguretat industrial i de pública concurrència**.

Quan un canvi normatiu pugui afectar el sistema d'informació o el compliment de l'ENS, es comunica a les persones responsables corresponents per valorar-ne l'impacte i adoptar les mesures necessàries.

7. Organització de la seguretat

L'organització de la seguretat s'articula mitjançant els rols ENS definits al Reial decret 311/2022, diferenciant les responsabilitats sobre la informació, els serveis, la seguretat i l'operació tècnica del sistema.

Els rols principals són els següents:

- **Responsable de la Informació**: determina els requisits de seguretat de la informació tractada, especialment en relació amb la seva confidencialitat, integritat, disponibilitat, autenticitat i traçabilitat. Participa en la valoració de la informació, la categorització del sistema i l'acceptació del risc residual que afecti la informació sota la seva responsabilitat.

- **Responsable del Servei**: determina els requisits de seguretat dels serveis prestats i valora l'impacte que tindria una interrupció, degradació o alteració del servei. Participa en la definició de prioritats de continuïtat, recuperació i tractament de riscos.
- **Responsable de Seguretat**: coordina, impulsa i supervisa la seguretat de la informació, vetllant per la implantació i el seguiment de les mesures ENS. Supervisa el compliment de la Política de Seguretat, la Declaració d'Aplicabilitat, l'anàlisi i tractament de riscos, la gestió d'incidents, les auditories i les accions de millora.
- **Responsable del Sistema**: s'encarrega de l'explotació, administració i control tècnic del sistema d'informació. Garanteix que les decisions de seguretat s'implanten correctament en la infraestructura, aplicacions, comunicacions, accessos, configuracions, actualitzacions, còpies de seguretat i procediments tècnics.

Així mateix, es constitueix un **Comitè de Seguretat de la Informació** com a òrgan de govern, coordinació i seguiment de la seguretat. Les seves funcions principals són supervisar l'aplicació d'aquesta Política, revisar riscos, incidents, auditories i plans d'acció, resoldre conflictes entre rols quan sigui necessari i impulsar la millora contínua de la seguretat.

La designació concreta de les persones responsables, la composició del Comitè de Seguretat i el funcionament detallat del model de govern s'estableixen als documents:

- **Designació de Rols, Òrgans i Responsabilitats ENS.**
- **Acta de Constitució del Comitè de Seguretat de la Informació.**

Atès que existeix un model tecnològic i de seguretat amb elements comuns i centralitzats, determinats rols, òrgans, procediments, controls i evidències poden ser compartits entre les entitats, sens perjudici que cada entitat mantingui les seves responsabilitats sobre la informació tractada i els serveis prestats en el seu àmbit.

El Comitè de Seguretat serà responsable de supervisar l'aplicació d'aquesta Política, revisar riscos, incidents, auditories i plans d'acció, resoldre conflictes entre rols quan sigui necessari i impulsar la millora contínua de la seguretat.

8. Tractament de dades personals

Les entitats incloses dins l'abast de la present Política tracten dades personals d'acord amb els seus respectius registres d'activitats de tractament, amb la normativa aplicable en matèria de protecció de dades i amb la documentació interna vigent de cada entitat en aquesta matèria.

Els riscos associats als tractaments s'han de valorar periòdicament i coordinar-se amb l'anàlisi de riscos ENS, especialment quan afectin la confidencialitat, la integritat, la disponibilitat, l'autenticitat o la traçabilitat de la informació.

Quan s'identifiquin tractaments d'alt risc, es durà a terme, quan correspongui, una Avaluació d'Impacte relativa a la Protecció de Dades —AIPD—. La implantació de mesures de seguretat es coordinarà amb els procediments de gestió de riscos, proveïdors, control d'accessos, continuïtat i resposta davant incidents.

La persona delegada de protecció de dades assessorarà i supervisarà els aspectes relatius al compliment de la normativa de protecció de dades, inclosa la gestió de les violacions de seguretat que afectin dades personals.

9. Gestió de riscos

Tots els sistemes subjectes a aquesta Política han de disposar d'una anàlisi de riscos adequada a la naturalesa de la informació tractada, els serveis prestats, els actius afectats, la categoria ENS aplicable i els requisits del sistema de gestió de seguretat de la informació d'acord amb la norma ISO/IEC 27001:2022.

L'anàlisi de riscos s'haurà de revisar:

- Com a mínim una vegada a l'any.
- Quan canviïn els serveis prestats o la informació tractada.
- Quan s'incorporin nous sistemes, aplicacions, proveïdors o serveis rellevants.
- Davant incidents de seguretat significatius.
- Davant vulnerabilitats crítiques o canvis rellevants en l'entorn tecnològic.
- Quan es modifiquin tractaments de dades personals o avaluacions d'impacte.

El Comitè de Seguretat farà el seguiment dels riscos i dels plans de tractament, prioritzant les accions necessàries per reduir els riscos no acceptables.

Les decisions rellevants es reflectiran en la Declaració d'Aplicabilitat, en el Pla de Tractament de Riscos, en l'anàlisi de riscos del SGSI i en les evidències corresponents.

10. Sistema de Gestió de la Seguretat de la Informació

Les entitats incloses estableixen, implanten, mantenen i milloren de manera contínua un Sistema de Gestió de la Seguretat de la Informació —SGSI— d'acord amb els requisits de la norma ISO/IEC 27001:2022 i de manera integrada amb l'Esquema Nacional de Seguretat.

El SGSI té com a finalitat assegurar que la seguretat de la informació es gestiona de forma sistemàtica, documentada i basada en riscos, incloent-hi la identificació d'actius, l'anàlisi i el tractament de riscos, la selecció de controls, la definició d'objectius de seguretat, la gestió d'incidents, l'avaluació de l'acompliment, l'auditoria interna, la revisió per la Direcció i la millora contínua.

L'aplicació dels controls de seguretat es documentarà mitjançant la Declaració d'Aplicabilitat, tenint en compte tant els requisits de l'ENS com els controls aplicables del SGSI d'acord amb la norma ISO/IEC 27001:2022.

La Direcció es compromet a proporcionar els recursos necessaris, promoure el compliment d'aquesta Política, donar suport a l'assoliment dels objectius de seguretat de la informació i revisar periòdicament l'eficàcia del SGSI.

11. Desenvolupament de la Política de Seguretat

Aquesta Política es desenvolupa i es complementa mitjançant el Sistema de Gestió de la Seguretat de la Informació —SGSI—, així com mitjançant normes, procediments, instruccions i registres específics, que inclouen, entre d'altres:

- Normativa de Seguretat.
- Control d'accessos.
- Còpies de seguretat i recuperació.
- Gestió d'incidents.
- Gestió de proveïdors.
- Gestió dels canvis.
- Normes d'ús.
- Inventari d'actius.
- Declaració d'Aplicabilitat.
- Anàlisi de riscos.
- Abast del SGSI.
- Metodologia d'anàlisi i tractament de riscos.
- Objectius de seguretat de la informació.
- Declaració d'Aplicabilitat ENS / ISO 27001:2022.
- Seguiment, mesurament, auditoria interna i revisió per la direcció.

La documentació associada estarà disponible per al personal que necessiti conèixer-la en funció de les seves responsabilitats i s'haurà de mantenir actualitzada al repositori documental definit.

12. Obligacions del personal

Tot el personal haurà de conèixer i complir aquesta Política, la **Normativa d'ús dels recursos TIC** i les normes de seguretat associades que resultin aplicables.

Les entitats incloses garantiran la difusió de la Política i de la normativa interna d'ús TIC, i promouran accions de formació i conscienciació en seguretat de la informació.

El personal haurà de:

- Utilitzar els sistemes d'informació d'acord amb les normes internes d'ús TIC i les instruccions de seguretat aplicables.
- Protegir les seves credencials i no compartir usuaris ni contrasenyes.
- Respectar el principi de mínim privilegi.
- Mantenir la confidencialitat de la informació a la qual tingui accés.
- Comunicar incidents, sospites d'incidents o usos indeguts dels sistemes.

- Complir les instruccions relatives a protecció de dades, seguretat, ús de dispositius, accés remot i tractament d'informació.
- Participar en les accions de formació o conscienciació que s'estableixin. Les persones que administrin, operin o gestionin sistemes TIC hauran de rebre formació adequada a les seves responsabilitats i actuar d'acord amb els procediments tècnics i de seguretat aplicables.

13. Tercers, proveïdors i prestadors de serveis

Quan les entitats incloses utilitzin serveis de tercers o permetin l'accés de proveïdors a informació, actius o sistemes inclosos en l'abast ENS i/o del SGSI, s'hauran d'establir els requisits de seguretat aplicables en funció del risc, la criticitat del servei i la informació tractada**.**

Els tercers i proveïdors hauran de complir les obligacions legals, contractuals i de seguretat que els siguin aplicables, incloent-hi, quan escaigui, els requisits de l'ENS, la normativa de protecció de dades i les condicions específiques establertes per l'organització.

En serveis al núvol, allotjament, suport tècnic, aplicacions externes, plataformes SaaS (Programari com a Servei) o serveis crítics, es tindran en compte els requisits de seguretat aplicables, les guies CCN-STIC corresponents i les evidències de seguretat disponibles del proveïdor.

Quan un proveïdor tracti dades personals per compte d'alguna de les entitats, s'haurà de formalitzar el corresponent contracte o acord d'encarregat del tractament, quan sigui aplicable.

Si algun requisit de seguretat no es pogués satisfer, la persona Responsable de Seguretat, amb la participació de les persones responsables afectades, valorarà el risc i proposarà les mesures de tractament oportunes. La continuïtat del servei o la contractació haurà de ser acceptada pels responsables corresponents quan existeixi un risc residual rellevant.

Per a l'ús de sistemes o serveis basats en intel·ligència artificial, s'haurà de valorar prèviament l'impacte en la seguretat, la protecció de dades, la confidencialitat, la integritat de la informació, el compliment normatiu i la dependència tecnològica.

Es procedirà a la selecció, avaluació i homologació de proveïdors, inclosos els proveïdors crítics, segons el que estableix el procediment de **Selecció, avaluació i homologació de proveïdors.**

14. Gestió d'incidents de seguretat

Les entitats incloses disposaran de procediments per a la gestió d'esdeveniments i incidents que puguin afectar la informació, els sistemes o els serveis inclosos en l'abast ENS i/o del SGSI. Concretament, s'actuarà d'acord amb el procediment de **Notificacions de les bretxes de seguretat.**

La gestió d'incidents haurà de permetre:

- Detectar i registrar esdeveniments i incidents.
- Classificar-ne la gravetat i l'impacte.
- Contenir-ne i mitigar-ne els efectes.
- Coordinar la resposta tècnica, funcional, jurídica i de protecció de dades quan correspongui.

- Comunicar els incidents a les persones responsables afectades.
- Notificar-los a les autoritats competents quan sigui exigible.
- Analitzar-ne les causes i definir accions correctives.
- Evitar recurrències.
- Mantenir evidències de la gestió realitzada**.**

Quan l'incident afecti dades personals, es coordinarà la resposta amb la persona delegada de protecció de dades i es valorarà la necessitat de notificació a l'autoritat de control i, si escau, a les persones afectades.

Els incidents rellevants es comunicaran al Comitè de Seguretat de la Informació.

15. Revisió de la Política de Seguretat de la Informació

La present Política serà revisada:

- Com a mínim una vegada a l'any.
- Quan es produeixin canvis rellevants en l'organització, els serveis, els sistemes, els proveïdors o l'abast ENS i/o del SGSI.
- Quan es produeixin incidents de seguretat significatius.
- Com a conseqüència d'auditories, revisions o canvis normatius.
- Quan el Comitè de Seguretat ho consideri necessari.

La revisió serà coordinada per la persona Responsable de Seguretat i elevada al Comitè de Seguretat per a la seva validació i aprovació per part de les Direccions corresponents

16. Aprovació

La present Política de Seguretat de la Informació és aprovada per les Direccions de les entitats incloses, que es comprometen a promoure'n el compliment, proporcionar els recursos necessaris i donar suport a la millora contínua de la seguretat de la informació.

El Prat de Llobregat, a 4 de juny de 2026

Cristina Rodríguez Portillo
Directora General de Fundesplai i
Presidenta del Consell d'Administració
de 7iTria

Víctor Hugo Martínez Buixeda
Direcció General Fundación Esplai
Ciudadanía Comprometida