Política de Seguretat de la Informació FPC

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Fundació Politècnica de Catalunya

Informació del document

Títol	Política de Seguretat de la Informació FPC
Codi	POL_SEG_01

Versió	Redactat / Revisat per	Aprovat per	Data aprovació	Data publicació
1.0	Esteve Miralles Nicolau / Gerard Campanera Mercè	Comitè de Seguretat de la Informació	27/03/2025	27/03/2025

Registre de canvis

Versió	Pàgines	Data de modificació	Motiu del canvi
1.0	14	27/03/2025	Versió inicial

ÍNDEX

1. INTRODUCCIÓ

La Fundació Politècnica de Catalunya (FPC), depèn dels sistemes de Tecnologies d'Informació i Comunicacions (TIC) per aconseguir els seus objectius, exercir les seves competències i prestar els serveis que té atribuïts. Aquests sistemes han de ser administrats amb diligència, prenent les mesures adequades per a protegir-los enfront de danys accidentals o deliberats que puguin afectar la disponibilitat, integritat o confidencialitat de la informació tractada o els serveis prestats.

L'objectiu de la seguretat de la informació és garantir la confidencialitat, integritat, autenticitat i traçabilitat de la informació i la prestació continuada dels serveis, actuant preventivament, supervisant l'activitat diària i reaccionant amb rapidesa als incidents.

Els sistemes TIC han d'estar protegits contra amenaces de ràpida evolució amb potencial per incidir a la confidencialitat, integritat, disponibilitat, ús previst i valor de la informació i els serveis. Per a defensar-se d'aquestes amenaces, es requereix una estratègia que s'adapti als canvis en les condicions de l'entorn per a garantir la prestació contínua dels serveis. Això implica que els departaments han d'aplicar les mesures mínimes de seguretat exigides per l'Esquema Nacional de Seguretat (ENS), així com realitzar un seguiment continu dels nivells de prestació de serveis, seguir i analitzar les vulnerabilitats reportades, i preparar una resposta efectiva als incidents per garantir la continuïtat dels serveis prestats.

Els diferents departaments han de cerciorar-se que la seguretat TIC és una part integral de cada etapa del cicle de vida del sistema, des de la seva concepció fins a la seva retirada de servei, passant per les decisions de desenvolupament o adquisició i les activitats d'explotació. Els requisits de seguretat i la valoració del seu cost, han de ser identificats i inclosos en la planificació, en la sol·licitud d'ofertes, i en plecs de licitació per a projectes de TIC.

2. MISSIÓ DE l'FPC

L'FPC, per a la gestió dels seus interessos i de les funcions i competències que té atribuïdes en diferents normes o convenis, promou activitats i presta serveis que contribueixen a satisfer les necessitats i aspiracions de la població. Per això posa a disposició d'aquesta la realització de tràmits en línia amb l'objectiu d'impulsar la tramitació electrònica dels procediments administratius, la millora en la prestació dels serveis.

La Missió de l'FPC és promoure i gestionar l'extensa oferta d'estudis de la UPC orientats al desenvolupament professional, així com crear entorns d'aprenentatge en què els professionals en enginyeria, arquitectura, ciència, puguin adaptar-se als canvis i aprendre al llarg de la vida per a contribuir a la construcció d'un món sostenible i just, amb esperit crític i capacitat per treballar en equips interdisciplinaris i multiculturals.

3. ABAST

Aquesta Política s'aplicarà als sistemes d'informació de l'FPC, que estan relacionats amb l'exercici de drets per mitjans electrònics, amb el compliment de deures per mitjans electrònics o amb l'accés a la informació o al procediment administratiu i que es troben dins de l'àmbit d'aplicació de l'ENS.

4. MARC NORMATIU

El marc legal i regulador que afecta el desenvolupament de les activitats i competències de l'FPC està constituït per normes jurídiques europees, estatals, autonòmiques i locals orientades a l'administració electrònica, a la ciberseguretat i seguretat de la informació en general, així com a la protecció de dades.

Les normes jurídiques que constitueixen aquest marc, es troben recollides en un registre disposat a aquest efecte.

També formen part del marc normatiu les restants normes aplicables a l'FPC, derivades de les anteriors o relacionades amb elles. Entre aquestes, estan incloses les instruccions tècniques de seguretat d'obligat compliment, publicades mitjançant resolució de la Secretaria d'Estat d'Administracions Públiques i aprovades pel Ministeri d'Hisenda i Administracions Públiques, a proposta del Comitè Sectorial d'Administració Electrònica i a iniciativa del Centre Criptològic Nacional (CCN) tal com s'estableix a l'ENS i les guies de seguretat del CCN.

El manteniment del citat registre, contenint el marc legal i regulador, és responsabilitat de l'FPC, que disposarà d'un procediment d'identificació de la legislació aplicable que tingui en compte els orígens a consultar, l'encarregat de fer-lo, el seu registre, etc.

5. COMPLIMENT DELS REQUISITS MÍNIMS DE SEGURETAT

l'FPC per aconseguir el compliment de l'ENS, que recull els principis bàsics i els requisits mínims de seguretat, ha implementat diverses mesures de seguretat proporcionals a la naturalesa de la informació i els serveis a protegir, tenint en compte la categoria dels sistemes afectats.

- **La seguretat com un procés integral i mínim privilegi.**

La seguretat s'entén com un procés integral constituït per tots els elements tècnics, humans, materials, jurídics i organitzatius, relacionats amb el sistema. L'aplicació de l'ENS a l'FPC estarà presidida per aquest principi, que exclou qualsevol actuació puntual o tractament conjuntural.

Es prestarà la màxima atenció a la conscienciació de les persones que intervenen en el procés i als seus responsables jeràrquics, per a evitar que, la ignorància, la falta d'organització i coordinació, o d'instruccions inadequades, constitueixin fonts de risc per a la seguretat.

Els sistemes d'informació han de dissenyar-se i configurar-se atorgant els mínims privilegis necessaris per al seu correcte acompliment, la qual cosa implica incorporar els següents aspectes:

a) El sistema proporcionarà la funcionalitat imprescindible perquè l'FPC aconsegueixi els seus objectius competencials o contractuals.
b) Les funcions d'operació, administració i registre d'activitat seran les mínimes necessàries, i s'assegurarà que només siguin desenvolupades per les persones autoritzades, sigui des d'emplaçaments o equips autoritzats; podent-se exigir, si és el cas, restriccions d'horari i punts d'accés facultats.
c) En un sistema d'explotació s'eliminaran o desactivaran, mitjançant el control de la configuració, les funcions que siguin innecessàries o inadequades per a la finalitat que es persegueix. L'ús ordinari del sistema ha de ser senzill i segur, de manera que una utilització insegura requereixi un acte conscient per part de l'usuari.
d) S'aplicaran guies de configuració de seguretat per a les diferents tecnologies, adaptades a la categorització del sistema, a aquest efecte d'eliminar o desactivar les funcions que siguin innecessàries o inadequades.

- **Vigilància contínua, revaluació periòdica i integritat, actualització del sistema i millora contínua del procés de seguretat.**

La vigilància contínua per part de l'FPC permetrà la detecció d'activitats o comportaments anòmals i la seva oportuna resposta.

L'avaluació permanent de l'estat de la seguretat dels actius permetrà mesurar la seva evolució, detectant vulnerabilitats i identificant deficiències de configuració.

Les mesures de seguretat es reavaluaran i actualitzaran periòdicament, adequant la seva eficàcia a l'evolució dels riscs i els sistemes de protecció, podent arribar a un replantejament de la seguretat, si fos necessari.

La inclusió de qualsevol element físic o lògic en el catàleg actualitzat d'actius del sistema, o la seva modificació, requerirà autorització formal prèvia.

L'avaluació i monitoratge permanents permetran adequar l'estat de seguretat dels sistemes ateses les deficiències de configuració, les vulnerabilitats identificades i les actualitzacions que els afectin, així com la detecció precoç de qualsevol incident que tingui lloc sobre aquests.

El procés integral de seguretat implantat haurà de ser actualitzat i millorat de manera contínua. Per a això, s'aplicaran els criteris i mètodes reconeguts en la pràctica nacional i internacional relatius a la gestió de la seguretat de les tecnologies de la informació.

- **Gestió de personal i professionalitat.**

Tot el personal, propi o aliè relacionat amb els sistemes d'informació de l'FPC, dins de l'àmbit de l'ENS, seran formats i informats dels seus deures, obligacions i responsabilitats en matèria de seguretat. La seva actuació serà supervisada per a verificar que se segueixen els procediments establerts.

El significat i abast de l'ús segur del sistema es concretarà i plasmarà en unes normes de seguretat que seran aprovades per la direcció o l'òrgan superior corresponent. D'igual manera, es determinaran els requisits de formació i experiència necessària del personal per al desenvolupament del seu lloc de treball.

La seguretat dels sistemes d'informació estarà atesa i serà revisada i auditada per personal qualificat, dedicat i instruït en totes les fases del seu cicle de vida: planificació, disseny, adquisició, construcció, desplegament, explotació, manteniment, gestió d'incidències i desmantellament.

De manera objectiva i no discriminatòria s'exigirà que les organitzacions que proporcionin serveis comptin amb professionals qualificats i amb uns nivells idonis de gestió i maduresa dels serveis prestats.

- **Gestió de la seguretat basada en els riscs, anàlisis i gestió de riscs.**

L'anàlisi i la gestió dels riscs serà part essencial del procés de seguretat i serà una activitat contínua i permanentment actualitzada.

La gestió dels riscs permetrà el manteniment d'un entorn controlat, minimitzant els riscs a nivells acceptables. La reducció a aquests nivells es realitzarà mitjançant una apropiada aplicació de mesures de seguretat, de manera equilibrada i proporcionada a la naturalesa de la informació tractada, dels serveis a prestar i dels riscs als quals estiguin exposats.

Aquesta gestió es realitzarà per mitjà de l'anàlisi i tractament dels riscs als quals està exposat el sistema. Sense perjudici del que es disposa en l'annex II, s'emprarà alguna metodologia reconeguda internacionalment. Les mesures adoptades per a mitigar o suprimir els riscs hauran d'estar justificades i, en tot cas, existirà una proporcionalitat entre elles i els riscs.

- **Incidents de seguretat, prevenció, detecció, reacció i recuperació.**

L'FPC disposa de procediments de gestió d'incidents de seguretat d'acord amb el que es preveu en l'article 33, a la Instrucció Tècnica de Seguretat corresponent, i de mecanismes de detecció, criteris de classificació, procediments d'anàlisis i resolució, així com de les vies de comunicació a les parts interessades.

La seguretat del sistema contemplarà les accions relatives als aspectes de prevenció, detecció i resposta, a fi de minimitzar les seves vulnerabilitats i aconseguir que les amenaces sobre el mateix no es materialitzin o que, en el cas de fer-lo, no afectin greument la informació que tracta o als serveis que presta.

Les mesures de prevenció podran incorporar components orientats a la dissuasió o a la reducció de la superfície d'exposició, han d'eliminar o reduir la possibilitat que les amenaces s'arribin a materialitzar.

Les mesures de detecció aniran adreçades a descobrir la presència d'un ciberincident.

Les mesures de resposta es gestionaran en temps oportú, estaran orientades a la restauració de la informació i els serveis que poguessin haver-se vist afectats per un incident de seguretat.

El sistema d'informació garantirà la conservació de les dades i informació en suport electrònic.

D'igual manera, el sistema mantindrà disponibles els serveis durant tot el cicle vital de la informació digital, a través d'una concepció i procediments que siguin la base per a la preservació del patrimoni digital.

- **Existència de línies de defensa i prevenció davant altres sistemes d'informació interconnectats.**

L'FPC ha implementat una estratègia de protecció del sistema d'informació constituïda per múltiples capes de seguretat, constituïdes per mesures organitzatives, físiques i lògiques, de tal forma que quan una capa ha estat compromesa permeti desenvolupar una reacció adequada enfront dels incidents que no han pogut evitar-se, reduint la probabilitat que el sistema sigui compromès en el seu conjunt i minimitzar l'impacte final sobre aquest.

Es protegirà el perímetre del sistema d'informació, especialment, quan el sistema de l'FPC es connecta a xarxes públiques, tal com es defineixen en la legislació vigent en matèria de telecomunicacions, reforçant-se les tasques de prevenció, detecció i resposta a incidents de seguretat.

En tot cas, s'analitzaran els riscs derivats de la interconnexió del sistema amb altres sistemes i es controlarà el seu punt d'unió.

- **Diferenciació de responsabilitats, organització i implantació del procés de seguretat.**

L'FPC ha organitzat la seva seguretat comprometent a tots els membres de l'entitat mitjançant la designació de diferents rols de seguretat amb responsabilitats clarament diferenciades, tal com es recull en l'apartat de "**MODEL DE GOVERNANÇA**" del present document.

- **Autorització i control dels accessos.**

L'FPC ha implementat mecanismes de control d'accés al sistema d'informació, limitant-lo als usuaris, processos, dispositius i altres sistemes d'informació, degudament autoritzats, i exclusivament a les funcions permeses.

- **Protecció de les instal·lacions.**

L'FPC ha implementat mecanismes de control d'accés físic, prevenint els accessos físics no autoritzats, així com els danys a la informació i als recursos, mitjançant perímetres de seguretat, controls físics i proteccions generals en àrees.

- **Adquisició de productes de seguretat i contractació de serveis de seguretat.**

Per a l'adquisició de productes o contractació de serveis de seguretat l'FPC tindrà en compte la utilització de forma proporcionada a la categoria del sistema i el nivell de seguretat determinat, aquells que tinguin certificada la funcionalitat de seguretat relacionada amb l'objecte de la seva adquisició.

Per a la contractació de serveis de seguretat s'atendrà a l'assenyalat quant a la professionalitat.

- **Protecció de la informació emmagatzemada i en trànsit i continuïtat de l'activitat.**

L'FPC prestarà especial atenció a la informació emmagatzemada o en trànsit a través dels equips o dispositius portàtils o mòbils, els dispositius perifèrics, els suports d'informació i les comunicacions sobre xarxes obertes, que hauran d'analitzar-se especialment per a aconseguir una adequada protecció.

S'aplicaran procediments que garanteixin la recuperació i conservació a llarg termini dels documents electrònics produïts pels sistemes d'informació compresos en l'àmbit d'aplicació del Reial Decret 311/2022, de 3 de maig, pel qual es regula l'ENS (Reial Decret), quan això sigui exigible.

Tota informació en suport no electrònic que hagi estat causa o conseqüència directa de la informació electrònica a la qual es refereix l'ENS, haurà d'estar protegida amb el mateix grau de seguretat que aquesta. Per a això, s'aplicaran les mesures que corresponguin a la naturalesa del suport, de conformitat amb les normes que resultin d'aplicació.

Els sistemes disposaran de còpies de seguretat i s'establiran els mecanismes necessaris per a garantir la continuïtat de les operacions en cas de pèrdua dels mitjans habituals.

- **Registre d'activitat i detecció de codi nociu.**

L'FPC amb el propòsit de satisfer l'objecte d'aquest Reial Decret, amb plenes garanties del dret a l'honor, a la intimitat personal i familiar i a la pròpia imatge dels afectats, i d'acord amb la normativa sobre protecció de dades personals, de funció pública o laboral, i altres disposicions que resultin d'aplicació, registrarà les activitats dels usuaris, retenint la informació estrictament necessària per a monitorar, analitzar, investigar i documentar activitats indegudes o no autoritzades, que permet identificar a cada moment a la persona que actua.

A fi de preservar la seguretat dels sistemes d'informació, garantint la rigorosa observança dels principis d'actuació de les institucions, i de conformitat amb el que es disposa en el Reglament General de Protecció de Dades i la resta de normativa sobre protecció de dades i el respecte als principis de limitació de la finalitat, minimització de les dades i limitació del termini de conservació enunciats enllà, l'FPC podrà, en la mesura estrictament necessària i proporcionada, analitzar les comunicacions entrants o sortints, i únicament per als fins de seguretat de la informació, de manera que sigui possible impedir l'accés no autoritzat a les xarxes i sistemes d'informació, detenir els atacs de denegació de servei, evitar la distribució

malintencionada de codi nociu així com altres danys a les avantdites xarxes i sistemes d'informació.

Per a corregir o, si és procedent, exigir responsabilitats, cada usuari que accedeixi al sistema d'informació haurà d'estar identificat de manera única, de manera que se sàpiga, en tot moment, qui rep drets d'accés, de quin tipus són aquests, i qui ha acomplert una determinada activitat.

Infraestructures i serveis comuns.

L'FPC tindrà en compte que la utilització d'infraestructures i serveis comuns de les administracions públiques, inclosos els compartits o transversals, facilitarà el compliment del que es disposa en l'ENS.

Perfils de compliment específics i acreditació d'entitats d'implementació de configuracions segures.

L'FPC tindrà en compte l'aplicació d'aquells perfils de compliment específics que siguin d'aplicació.

6. MODEL DE GOVERNANÇA

Per a garantir el compliment de l'ENS i establir l'organització de la seguretat de la informació en l'organització, es designen rols de seguretat i es constitueix un Comitè de Seguretat de la informació.

ROLS O PERFILS DE SEGURETAT

Per a garantir el compliment i l'adaptació de les mesures exigides reglamentàriament, s'han creat rols o perfils de seguretat i s'han designat els càrrecs o òrgans que els ocuparan, de la següent manera:

- **Responsable/s d'Informació**: Director/a de Creixement i Cap d'Aprenentatge
- **Responsable dels Serveis**: Director/a de Creixement i Cap d'Aprenentatge
- **Responsable de Seguretat**: Cap de Sistemes d'Informació
- **Responsable del Sistema**: Responsable del Sistema

COMITÈ DE SEGURETAT DE LA INFORMACIÓ

S'ha constituït un Comitè de Seguretat de la Informació, com a òrgan col·legiat, i està format pels següents membres:

- **President/a**: Direcció executiva
- **Secretari/a**: Cap d'Administració i Control
- **Vocals**:

  - **Responsable d'Informació**.
  - **Responsable del Servei**.
  - **Responsable de Seguretat**.
  - **Responsable del Sistema**.
- **Delegat de Protecció de dades (DPD)**: Cap d'Assessoria Jurídica, amb funcions d'assessorament i supervisió en matèria de protecció de dades.

Els Responsables de la Informació i del Servei seran convocats en funció dels assumptes a tractar.

Així mateix, i amb caràcter opcional, es podran incorporar als treballs del Comitè grups de treball especialitzats, siguin de caràcter intern, extern o mixt.

Els membres del Comitè seran renovats cada **sis anys** o en ocasió de vacant.

RESPONSABILITATS ASSOCIADES A L'ESQUEMA NACIONAL DE SEGURETAT

A continuació, es detallen i s'estableixen les funcions i responsabilitats de cadascun dels rols de seguretat de l'ENS:

Funcions del Comitè de Seguretat de la Informació

Les funcions pròpies d'un Comitè de Seguretat de la Informació són les següents:

- Atendre les sol·licituds, en matèria de seguretat de la informació, de l'Administració i dels diferents rols de seguretat i/o àrees informant regularment de l'estat de la seguretat de la informació.
- Assessorar en matèria de seguretat de la informació.
- Resoldre els conflictes de responsabilitat que puguin aparèixer entre les diferents unitats administratives.
- Promoure la millora contínua del sistema de gestió de la seguretat de la informació. Per a això s'encarregarà de:
  - Coordinar els esforços de les diferents àrees en matèria de seguretat de la informació, per a assegurar que aquests siguin consistents, alineats amb l'estratègia decidida en la matèria, i evitar duplicitats.
  - Proposar plans de millora de la seguretat de la informació, amb la seva dotació pressupostària corresponent, prioritzant les actuacions en matèria de seguretat quan els recursos siguin limitats.
  - Vetllar perquè la seguretat de la informació es tingui en compte en tots els projectes des de la seva especificació inicial fins a la seva posada en operació. En particular, haurà de vetllar per la creació i utilització de serveis horitzontals que redueixin duplicitats i donin suport a un funcionament homogeni de tots els sistemes TIC.
  - Realitzar un seguiment dels principals riscs residuals assumits per l'Administració i recomanar possibles actuacions respecte d'ells.
  - Realitzar un seguiment de la gestió dels incidents de seguretat i recomanar possibles actuacions respecte d'ells.

- Elaborar i revisar regularment la Política de Seguretat de la Informació per a la seva aprovació per l'òrgan competent.
- Elaborar la normativa de seguretat de la informació per a la seva aprovació.
- Verificar els procediments de seguretat de la informació i altra documentació per a la seva aprovació.
- Elaborar programes de formació destinats a formar i sensibilitzar al personal en matèria de seguretat de la informació i en particular en matèria de protecció de dades de caràcter personal.
- Elaborar i aprovar els requisits de formació i qualificació d'administradors, operadors i usuaris des del punt de vista de seguretat de la informació.
- Promoure la realització de les auditories periòdiques ENS i de protecció de dades que permetin verificar el compliment de les obligacions en matèria de seguretat de la informació.

Funcions del Responsable d'Informació

- Establir i aprovar els requisits de seguretat aplicables al servei i la informació dins del marc establert en l'annex I de l'ENS.
- Acceptar els nivells de risc residual que afectin el Servei i a la Informació.

Funcions del Responsable de Seguretat

- Mantenir i verificar el nivell adequat de seguretat de la informació tractada i dels serveis electrònics prestats pels sistemes d'informació.
- Promoure la formació i conscienciació en matèria de seguretat de la informació.
- Designar responsables de l'execució de l'anàlisi de riscs, de la declaració d'aplicabilitat, identificar mesures de seguretat, determinar configuracions necessàries, elaborar documentació del sistema.
- Proporcionar assessorament per a la determinació de la categoria del sistema, en col·laboració amb el Responsable del Sistema.
- Participar en l'elaboració i implantació dels plans de millora de la seguretat i arribat el cas en els plans de continuïtat, procedint a la seva validació.
- Gestionar les revisions externes o internes del sistema.
- Gestionar els processos de certificació.
- Elevar a la Direcció l'aprovació de canvis i altres requisits del sistema.

Funcions del Responsable del Sistema

- Paralitzar o donar suspensió a l'accés a informació o prestació de servei si té el coneixement que aquests presenten deficiències greus de seguretat.
- Desenvolupar, operar i mantenir el sistema d'informació durant tot el seu cicle de vida.
- Elaborar els procediments operatius necessaris.
- Definir la tipologia i la gestió del sistema d'informació establint els criteris d'ús i els serveis disponibles en aquest.
- Cerciorar-se que les mesures específiques de seguretat s'integrin adequadament dins del marc general de seguretat.

- Prestar al Responsable de Seguretat de la informació assessorament per a la determinació de la categoria del sistema.
- Col·laborar, si així se li requereix, en l'elaboració i implantació dels plans de millora de la seguretat i, arribat el cas, en els plans de continuïtat.
- Dur a terme les funcions de l'administrador de la seguretat del sistema:
  - La gestió, configuració i actualització, en el seu cas, del maquinari i programari en els quals es basen els mecanismes i serveis de seguretat.
  - La gestió de les autoritzacions concedides als usuaris del sistema, en particular els privilegis concedits, incloent-hi el monitoratge de l'activitat desenvolupada en el sistema i la seva correspondència amb l'autoritzat.
  - Aprovar els canvis en la configuració vigent del sistema d'informació.
  - Assegurar que els controls de seguretat establerts es compleixen estrictament.
  - Assegurar que són aplicats els procediments aprovats per a gestionar el sistema d'informació.
  - Supervisar les instal·lacions de maquinari i programari, les seves modificacions i millores per a assegurar que la seguretat no està compromesa i que en tot moment s'ajusten a les autoritzacions pertinents.
  - Monitorar l'estat de seguretat proporcionat per les eines de gestió d'esdeveniments de seguretat i mecanismes d'auditoria tècnica.

PROCEDIMENTS DE DESIGNACIÓ

La designació dels Responsables identificats en aquesta Política ha estat realitzada per la Direcció i comunicada a les parts afectades a través dels documents de nomenament i actes corresponents.

Els rols de seguretat seran revisats cada **sis anys**, en el cas que existeixi una vacant la mateixa haurà de ser coberta en el termini d'un mes, seguint el mateix procediment.

RESOLUCIÓ DE CONFLICTES

Si hi hagués conflicte entre els Responsables, serà resolt pel Comitè de Seguretat de la Informació.

7. DADES DE CARÀCTER PERSONAL

Quan els sistemes d'informació tractin dades personals, els hi serà d'aplicació la normativa vigent en matèria de protecció de dades, així com els criteris que estableixin les autoritats de control competents. En aquests casos, de forma prèvia a la realització de les operacions que comportin tractament de dades personals, l'FPC elaborarà una anàlisi de riscos o una avaluació d'impacte relativa a la protecció de dades amb l'assessorament del seu delegat/da de protecció de dades. D'aquesta manera, l'FPC determinarà les mesures i els mecanismes necessaris per afrontar els

riscos detectats i garantir-ne la protecció. A aquests efectes, també s'haurà de tenir en compte la normativa interna de l'FPC en matèria de protecció de dades.

8. DESENVOLUPAMENT DE LA POLÍTICA DE SEGURETAT DE LA INFORMACIÓ

El compliment dels objectius marcats en aquesta Política de Seguretat es duu a terme mitjançant el desenvolupament de documentació que constitueix les normes i procediments de seguretat associats al compliment de l'ENS. Per a la seva organització s'ha definit una norma per a la gestió de la documentació, que estableix les directrius per a l'organització, gestió i accés.

La revisió anual de la present Política correspon al Comitè de Seguretat de la Informació, proposant en cas que sigui necessari millores d'aquesta, per a la seva aprovació per part del mateix òrgan que la va aprovar inicialment.

9. TERCERES PARTS

Quan es presti serveis a altres organismes, o es manegui informació d'altres organismes, se'ls farà partícips d'aquesta Política de Seguretat de la Informació.

L'FPC definirà i aprovarà els canals per a la coordinació de la informació i els procediments d'actuació per a la reacció davant incidents de seguretat, així com la resta de les actuacions que l'FPC dugui a terme en matèria de seguretat en relació amb altres organismes.

Quan l'FPC utilitzi serveis de tercers o cedeixi informació a tercers, se'ls farà partícips d'aquesta Política de Seguretat i de la normativa de seguretat existent que concerneixi aquests serveis o informació. Aquesta tercera part quedarà subjecta a les obligacions establertes en l'esmentada normativa, podent desenvolupar els seus propis procediments operatius per a satisfer-la. S'establiran procediments específics de comunicació i resolució d'incidències.

Es garantirà que el personal de tercers estigui adequadament conscienciat en matèria de seguretat, almenys al mateix nivell que l'establert en aquesta Política de Seguretat.

D'igual manera, tenint en compte l'obligació de complir amb el que es disposa en les Instruccions Tècniques de Seguretat recollida en la Disposició addicional segona (Desenvolupament de l'Esquema Nacional de Seguretat) del Reial Decret 311/2022, de 3 de maig, pel qual es regula l'ENS, i en consideració a la Instrucció Tècnica de Seguretat de conformitat amb l'Esquema Nacional de Seguretat, on s'estableix que els operadors del sector privat que prestin serveis o proveeixin solucions a les entitats públiques, als quals resulti exigible el compliment de l'ENS, hauran d'estar en condicions d'exhibir la corresponent Declaració de Conformitat amb l'ENS quan es tracti de sistemes de categoria BÀSICA, o la Certificació de Conformitat amb l'ENS, quan es tracti de sistemes de categories MITJANA o ALTA.

Quan algun aspecte d'aquesta Política de Seguretat no pugui ser satisfet per una tercera part segons es requereix en els paràgrafs anteriors, es requerirà un informe

del Responsable de Seguretat que precisi els riscs en què s'incorre i la manera de tractar-los. Aquest informe haurà de ser aprovat pels responsables d'informació i els serveis, amb caràcter previ a l'inici de la relació amb la tercera part.

10. APROVACIÓ I ENTRADA EN VIGOR

Text aprovat el dia 27 de març de 2025 pel Comitè de Seguretat de la Informació de l'FPC.

Aquesta Política de Seguretat de la Informació, serà efectiva des d'aquesta data i fins que sigui reemplaçada per una nova Política.