



Norma d'ús dels mitjans electrònics

POL_SEG_02



CONTROL DE SIGNATURES

Informació del document

Títol	Protocol de Manteniment i Actualització
Codi	POL_SEG_02

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	15	27/03/2025	Versió inicial



ÍNDEX

1. OBJECTIU	4
2. ÀMBIT I VIGÈNCIA	4
3. COMPLIMENT AMB ELS REQUISITS LEGALS I ESTÀNDARDS DE SEGURETAT	4
4. DESCRIPCIÓ	5
4.1 NORMES GENERALS	5
4.2 ÚS D'EQUIPAMENT INFORMÀTIC	5
4.2.1 Equips portàtils i dispositius mòbils	6
4.2.2 Suports d'informació	6
4.3 ACCÉS A SISTEMES D'INFORMACIÓ	7
4.4 ÚS DE LA INFORMACIÓ I DADES TRACTADES	8
4.4.1 Lloc de treball net	8
4.4.2 Neteja de metadades	9
4.4.3 Confidencialitat, protecció de dades personals i deure de secret	9
4.4.4 Documentació impresa	10
4.5 ACCÉS A INTERNET	10
4.6 ÚS DEL CORREU ELECTRÒNIC	11
4.7 PÈRDUA DE VINCULACIÓ AMB L'ENTITAT	13
4.8 INCIDENTS DE SEGURETAT	13
4.9 FORMACIÓ I CONSCIENCIACIÓ	13
4.10 CONTROL I MONITORATGE	13
5. DIFUSIÓ	14
6. GESTIÓ DE LA DOCUMENTACIÓ	14
7. INCOMPLIMENT	14

1. OBJECTIU

La present normativa té per objecte establir els criteris i les regles d'ús que s'han d'observar per a l'adequada utilització dels mitjans electrònics que la Fundació Politècnica de Catalunya (FPC) posa a disposició del personal per a l'exercici de les seves funcions, així com informar dels mitjans establerts per l'FPC, per tal de portar a terme el seu control i seguiment.

La finalitat principal d'aquesta normativa és protegir la informació de l'FPC i garantir el bon funcionament dels serveis, assegurant un ús adequat dels dispositius digitals i de la infraestructura informàtica i de comunicacions, vetllant pel compliment de la legislació vigent.

És fonamental que tots els empleats de l'FPC que utilitzen equipament informàtic i accedeixin o tractin informació de caràcter personal per a l'execució de les seves funcions i tasques coneguin aquesta norma.

2. ÀMBIT I VIGÈNCIA

Mitjançant la present normativa, l'FPC estableix la regulació de l'ús dels mitjans electrònics, a través de l'establiment de mesures de compliment obligatori per a tot el personal, quedant subjectes a aquesta, així com als principis morals i ètics en la utilització dels recursos posats a disposició.

La normativa és d'obligat compliment per a tot el personal de l'FPC, així com a aquell personal de tercers que empli els sistemes d'informació de l'FPC. En endavant s'utilitzarà el terme "usuari" per tal de referir-se al personal propi i al de tercers.

La normativa ha estat aprovada pel Comitè de seguretat, entrarà en vigor l'endemà de la seva aprovació i es mantindrà vigent fins a la pròxima versió aprovada d'aquesta.

3. COMPLIMENT AMB ELS REQUISITS LEGALS I ESTÀNDARDS DE SEGURETAT

El present document proporciona cobertura als objectius de control que s'enumeren tot seguit.

Aquests són recollits a la legislació vigent aplicable en matèria de seguretat de la informació i les bones pràctiques reconegudes:

- Reial decret 311/2022, 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat:
 - o Annex II – [Normativa de seguretat](#)

4. DESCRIPCIÓ

4.1 NORMES GENERALS

Els usuaris utilitzaran els mitjans electrònics facilitats per l'FPC per a fins professionals orientats al compliment de les seves obligacions de servei i laborals. No obstant això, els usuaris podran fer un ús privat dels mitjans electrònics corporatius, sempre que es faci de manera excepcional, no abusiva i circumstancial a l'efecte d'atendre assumptes inexcusables o que facilitin la conciliació de la vida familiar i laboral.

Amb caràcter general, els usuaris no podran utilitzar mitjans electrònics de la seva propietat per desenvolupar les tasques encomanades. L'ús de dispositius propietat del personal haurà d'estar formalment autoritzat per l'FPC i haurà de complir amb les condicions de seguretat que l'FPC estableixi per a garantir la protecció de la informació i dels sistemes d'informació.

Els usuaris hauran de seguir els criteris generals de seguretat i les regles d'ús segur en la utilització dels mitjans electrònics, que estan desenvolupats i detallats en aquesta norma i en la normativa corporativa de seguretat establerta per l'FPC.

4.2 ÚS D'EQUIPAMENT INFORMÀTIC

Amb relació a l'equipament informàtic (incloent-hi equips de sobretaula, portàtils i dispositius mòbils) que proporcioni l'FPC als usuaris, caldrà que tinguin en compte les següents obligacions:

- Excepte autorització expressa no disposaran de privilegis d'administrador sobre els equips.
- Únicament els usuaris autoritzats podran distribuir, instal·lar o desinstal·lar programari i maquinari, o modificar la configuració de qualsevol dels equips.
- No podran desactivar o modificar els paràmetres de configuració del programari antivirus o de protecció de codi maliciós que s'executa automàticament per protegir la informació i el sistema.
- Quan sigui necessari instal·lar equips que no hagin estat proveïts per l'FPC hauran de sol·licitar autorització prèvia.
- Activaran el mecanisme de bloqueig segur de pantalla quan l'equip hagi de romandre desatès.
- S'abstindran d'alterar o modificar els equips i, en concret, accedir físicament a l'interior per tal de manipular-los.
- S'abstindran de fer ús dels equips informàtics assignats a altres usuaris sense el seu coneixement, llevat que compti amb l'autorització del responsable competent.
- En finalitzar la jornada laboral haurà de tancar l'equip. Aquesta mesura serà d'aplicació sempre que no es tracti d'equips dels quals es requereixi un funcionament continu, com components d'algun sistema/servei que exigeixi continuïtat.

4.2.1 Equips portàtils i dispositius mòbils

Per als equips portàtils i els dispositius mòbils, a més de les normes generals, els usuaris hauran de tenir en compte les següents normes específiques per aquests equips:

- Aquests equips estaran, en tot moment sota la custòdia de l'usuari que els utilitzi, que serà la responsable d'adoptar les mesures necessàries per a evitar danys, pèrdua o sostracció i l'accés a ells per part de persones no autoritzades.
- La pèrdua o sostracció d'aquests equips s'ha de notificar immediatament per a l'adopció de les mesures que corresponguin.
- S'ha de sol·licitar autorització quan s'utilitzin per a connectar-se remotament a través de xarxes que no estiguin sota el control de l'FPC o que no hagin estat autoritzades, autorització que es farà extensible també als serveis als quals s'accedeix. Aquestes connexions remotes es realitzaran només amb connexions VPN segures que els responsables posin a la disposició dels usuaris.
- Quan es modifiquin les circumstàncies professionals (finalització de la tasca encomanada, cessament en el càrrec, etc.) que van originar el lliurament d'un recurs informàtic mòbil, l'usuari el retornarà, a fi de portar a terme l'esborrament segur de la informació emmagatzemada i restaurar l'equip al seu estat original perquè pugui ser assignat a una nova persona o perquè es porti a terme la seva destrucció segura.

4.2.2 Suports d'informació

Com a norma general, l'ús de suports d'emmagatzematge extraïbles (memòries USB, discos durs, etc.) no està autoritzat. Per a la seva utilització s'haurà de disposar de la deguda autorització.

En el cas que a l'usuari se li autoritzi l'ús d'aquest tipus de suports, les normes a seguir són les següents:

- Com a norma general, s'utilitzaran els suports extraïbles proporcionats per l'FPC, destinats a ús exclusivament professional, com a eina de transport puntual de fitxers i no com a eina d'emmagatzematge.
- L'ús de suports d'emmagatzematge extraïbles propis de l'usuari no està autoritzat, tret que es disposi de la deguda autorització.
- L'ús de suports d'emmagatzematge extraïbles no està autoritzat per a l'emmagatzematge de dades personals, tret que es disposi de la deguda autorització.
- Els suports d'emmagatzematge hauran de guardar-se en llocs segurs, a fi de prevenir robatoris o l'accés de tercers no autoritzats.
- El transport dels suports d'emmagatzematge fora de les instal·lacions de l'FPC haurà de ser realitzat exclusivament per usuaris autoritzats, autorització que haurà de referir-se a la informació que aquest conté. En

aquest cas s'haurà d'enviar una sol·licitud perquè se l'assessori sobre les mesures de seguretat que serà necessari implementar.

- Els suports d'emmagatzematge que, per obsolescència o degradació, perdin la seva utilitat, i especialment aquells que continguin dades de caràcter personal, hauran de ser eliminats de manera segura per a evitar accessos a aquesta informació.
- Per a la reutilització de suports d'emmagatzematge, per a altres finalitats diferents de les que van originar el seu ús, haurà de sol·licitar-se un esborrament segur d'aquest.

4.3 ACCÉS A SISTEMES D'INFORMACIÓ

Per a accedir als sistemes d'informació és necessari tenir assignat prèviament un compte d'usuari. L'alta dels usuaris serà sol·licitada i autoritzada d'acord amb les polítiques de l'FPC i el procediment de gestió d'usuaris. L'autorització de l'accés establirà el perfil necessari amb el qual es configurin les funcionalitats i privilegis disponibles en les aplicacions segons les competències de cada persona, adoptant una política d'assignació de privilegis mínims necessaris per a la realització de les funcions encomanades.

Els usuaris disposaran de credencials personals d'accés (identificador i contrasenya, i si fos necessari certificat electrònic, etc.) per a l'accés als sistemes d'informació de l'FPC emprant la xarxa segura, protegida amb els serveis de seguretat destinats a aquest efecte, sent responsables de la seva custòdia i de tota activitat relacionada amb l'ús del seu accés autoritzat, respecte dels quals haurà d'observar les següents mesures:

- L'identificador d'usuari és únic per a cada persona, intransferible i independent de l'equip des del qual es realitza l'accés.
- Els usuaris no han de revelar o lliurar, en cap concepte, les seves credencials d'accés a una altra persona, ni tan sols als administradors, ni mantenir-les per escrit a la vista o a l'abast de tercers. D'igual mode, no han d'utilitzar cap accés d'una altra persona, encara que disposin de l'autorització del seu titular.
- No utilitzar en l'àmbit personal les credencials corporatives en comptes de correu personal, xarxes socials i altres aplicacions.
- Si una persona té sospites que les seves credencials són utilitzades per una altra persona, ha de comunicar-ho immediatament.
- Els usuaris han d'utilitzar contrasenyes segures, d'acord amb la política establerta a l'FPC, no han d'estar compostes únicament per paraules del diccionari o altres fàcilment predictibles o associables a l'usuari (noms de familiars o mascotes, números de telèfon, dates o en general informació biogràfica de l'usuari).
- Els sistemes que així ho permetin, forçaran el canvi de la contrasenya periòdicament d'acord amb la normativa de l'FPC. En els sistemes d'informació que no sigui possible, serà responsabilitat dels usuaris procedir al seu canvi manual respectant la periodicitat establerta.

Quan s'acabi d'utilitzar un sistema d'informació es tancarà la sessió, protegint l'accés a les dades d'aquest.

4.4 ÚS DE LA INFORMACIÓ I DADES TRACTADES

La informació s'ha d'emmagatzemar en les eines informàtiques o els serveis corporatius que l'FPC posa a disposició dels usuaris.

Està prohibit utilitzar, copiar o transmetre informació continguda en els sistemes informàtics per a ús privat o qualsevol altre diferent del servei al qual està destinada.

L'usuari s'abstindrà de copiar la informació continguda en els fitxers que emmagatzemen dades de caràcter personal o un altre tipus d'informació de l'FPC, en els dispositius digitals de la seva propietat, memòries USB o a qualsevol altre suport informàtic, llevat que sol·liciti autorització al Responsable de Seguretat i s'adoptin les mesures de seguretat corresponents.

L'usuari s'ha d'abstenir d'accedir a qualsevol informació que no sigui estrictament necessària per al desenvolupament de les seves funcions o tasques dins de l'FPC.

L'usuari ha de restringir a tercers (familiars, amistats o qualsevol altre) l'accés als arxius o fitxers, titularitat de l'FPCi disposats per raó única de les funcions o tasques exercides en aquesta.

4.4.1 Lloc de treball net

El lloc de treball és, per la seva pròpia naturalesa, una zona vulnerable, per la qual cosa, actius com la informació en suport paper que es mantingui a les taules, calaixos o la informació accessible a través dels dispositius situats en ell, estan sotmesos a importants riscos com la pèrdua, el robatori o la fuga d'informació, entre altres amenaces.

Per evitar possibles incidències respecte a la informació:

- Els llocs de treball romandran buits, nets i ordenats, amb els materials i recursos imprescindibles per a la realització de les tasques oportunes que es portin a terme en cada moment.
- En el moment que un recurs, material o informació hagi deixat d'utilitzar-se per a la tasca que s'estigui realitzant, s'ha de retirar en un calaix, armari, prestatgeria o a una sala separada, de manera que quedi tancat amb clau o amb un altre mecanisme similar que eviti els accessos no autoritzats, la pèrdua, el robatori o la fugida d'informació.
- En finalitzar la jornada de treball, tota la informació i dispositius romandran en els armaris, calaixos i sales disponibles per garantir-ne la seguretat mentre s'estigui fora de l'horari laboral. Els equips poden romandre a les taules sempre que s'adoptin altres mesures com ara cadenats o docks amb clau, sempre que això impedeixi que persones no autoritzades puguin accedir-hi o sostreure'ls.
- S'ha d'evitar, en la mesura del possible, treballar amb documentació en paper, així com vetllar que no quedin a la vista de persones no autoritzades anotacions o post-its sobre la taula o la pantalla que puguin contenir informació d'interès. La informació en paper que ja no sigui d'utilitat

s'eliminarà amb trituradores de paper o es dipositarà als contenidors del servei de destrucció posats a disposició del personal.

- S'ha de tenir especial cura de no deixar anotacions amb credencials corporatives i contrasenyes, així com targetes criptogràfiques que puguin permetre que persones no autoritzades accedeixin a informació i recursos de l'FPC.
- En cap cas es deixarà informació i suports que continguin informació delicada a la vista sense cap mena de seguretat.

4.4.2 Neteja de metadades

Tots els arxius electrònics (documents ofimàtics, fulls de càlcul, imatges, etc.) disposen, en les seves propietats d'una sèrie de dades ocultes i/o metadades. Aquestes proporcionen informació molt variada sobre l'arxiu, com per exemple la data de creació, ubicació on va ser creat, l'autor o l'última modificació, entre d'altres. Les metadades contingudes en els arxius poden arribar a afectar la seguretat i la confidencialitat de la informació, a més a més de la imatge de l'FPC.

Per aquest motiu, tot arxiu que hagi de ser difós internament, remès electrònicament a un tercer o publicat a Internet (pàgina web, seu electrònica, etc.), serà revisat amb anterioritat per procedir amb la supressió de dades ocultes i/o metadades que continguin informació que no hagi de ser revelada al receptor, d'acord amb el previst en el procediment de neteja manual de metadades.

4.4.3 Confidencialitat, protecció de dades personals i deure de secret

La informació continguda en els sistemes d'informació de l'FPC és responsabilitat d'aquesta, per la qual cosa els usuaris han d'abstenir-se de comunicar, divulgar, distribuir o posar en coneixement o a l'abast de tercers (externs o interns no autoritzats) aquesta informació, excepte si es disposa d'autorització expressa de la mateixa FPC. A més, haurà de tenir en compte les següents premisses:

- Tots els usuaris que, per raó de la seva activitat professional, haguessin tingut accés a informació gestionada per l'FPC (documents, metodologies, claus, anàlisis, programes, etc.) hauran de mantenir sobre ella, per temps indefinit, una absoluta reserva.
- Els usuaris només podran accedir amb les degudes autoritzacions a aquella informació necessària per a l'acompliment de les seves tasques. En tot cas, no haurà d'accedir a informació sense les degudes autoritzacions.
- Tota informació continguda en els sistemes d'informació de l'FPC o que circuli per les seves xarxes de comunicacions ha de ser utilitzada únicament per al compliment de les funcions que té encomanades l'usuari.
- La informació obtinguda o creada durant la relació laboral amb l'FPC, és propietat de l'FPCi, per tant, no podrà ser retinguda, reenviada, ni eliminada sense disposar de l'autorització prèvia i formal del propietari de la informació.
- Els drets d'accés dels usuaris a la informació i als sistemes d'informació que la tracten deuran sempre atorgar-se sobre la base dels principis de "mínim



privilegi”, “necessitat de conèixer i responsabilitat de compartir” i “capacitat d'autoritzar”.

- La informació que contingui dades de caràcter personal quedarà afectada també per la normativa vigent en matèria de protecció de dades personals. El personal està obligat a complir amb aquesta normativa i guardar secret sobre les dades personals, deure que es mantindrà de manera indefinida fins i tot més enllà de la relació laboral o professional amb l'FPC.
- S'ha de comunicar qualsevol necessitat relacionada amb el tractament de dades personals (nous tractaments, modificació o supressió de dades, noves utilitzacions amb finalitats diferents, comunicacions) als canals establerts o a la persona delegada de protecció de dades.

4.4.4 Documentació impresa

Hauran d'utilitzar-se les impressores de xarxa i les fotocopiadores corporatives que l'FPC posa a disposició dels usuaris.

En relació amb els sistemes de còpia i impressió, i documentació impresa, els usuaris han de seguir les següents directrius:

- Els documents, amb caràcter general, es generaran en format electrònic, podent digitalitzar aquells que no siguin susceptibles de no ser generats en aquest format.
- Quan s'imprimeixin documents, aquests hauran de romandre el menor temps possible en les safates de sortida de les impressores, per a evitar que terceres persones puguin accedir a aquesta.
- En la realització de còpies i/o escaneig de documents, caldrà tenir cura de retirar els originals.
- En cas de trobar documentació en un sistema de còpia o impressió, l'usuari intentarà localitzar el propietari perquè procedeixi a la seva recollida immediata. En cas de desconèixer el propietari o no estar localitzable, ho posarà immediatament en coneixement.
- Per a evitar un ús excessiu dels recursos, millorant l'impacte mediambiental en la generació de documents en paper, i per motius de seguretat, abans d'imprimir documents, l'usuari ha d'assegurar-se que és absolutament necessari fer-ho.

4.5 ACCÉS A INTERNET

L'accés corporatiu a Internet és un recurs centralitzat que l'FPC posa a la disposició dels usuaris, com a eina necessària per a l'accés a continguts i recursos d'Internet i com a suport per l'acompliment de la seva activitat professional. L'FPC vetllarà pel bon ús de l'accés a Internet, tant des del punt de vista de l'eficiència i productivitat de l'usuari, com des dels riscos de seguretat associats al seu ús. Les normes d'ús són les següents:

- La connexió a Internet per la prestació del servei s'ha de fer, preferentment, a través de les xarxes corporatives proporcionades per l'FPC. En cas d'utilitzar

xarxes WIFI privada per a la connexió a Internet, caldrà que aquesta requereixi contrasenya per establir connexió.

- Caldrà abstenir-se de connectar-se a Internet utilitzant xarxes WIFI públiques no vinculades a l'FPC.
- Només es podrà accedir a Internet mitjançant els navegadors subministrats i configurats per l'FPC. No podrà alterar-se la seva configuració, ni utilitzar un navegador alternatiu, sense disposar de la deguda autorització.
- El sistema que proporciona el servei de navegació podrà disposar de filtres d'accés que bloquegin l'accés a pàgines web amb continguts inadequats, programes lúdics de descàrrega massiva o pàgines potencialment insegures o que continguin virus o codi nociu.
- Els usuaris no poden connectar els dispositius digitals de la seva propietat fent ús de la connexió a Internet corporativa.
- Haurà de notificar-se qualsevol anomalia (redirecció a pàgines sol·licitades, avís de lloc no segur en pàgines habitualment utilitzades, etc.) detectada en l'ús de l'accés a Internet, així com la sospita de possibles problemes o incidents de seguretat relacionats amb aquest accés.

Es consideren usos prohibits, que impliquen un risc de seguretat, les següents actuacions:

- Consultar pàgines web que no tinguin relació directa amb les funcions i tasques assignades, incloent-hi pàgines web de vídeos en línia.
- La descàrrega de programes informàtics sense l'autorització prèvia o fitxers amb contingut nociu que suposin una font de riscos per a l'FPC. En tot cas ha d'assegurar-se que el lloc web visitat és de confiança.
- L'accés, la descàrrega i/o l'emmagatzematge en qualsevol suport, de continguts il·legals, nocius, inadequats o que atemptin contra la moral i els bons costums.
- L'accés a recursos i pàgines web, o la descàrrega de programes o continguts que vulnerin la legislació en matèria de Propietat Intel·lectual.
- La utilització d'aplicacions o eines (especialment, l'ús de programes d'intercanvi d'informació, P2P) per a la descàrrega massiva d'arxius, programes o un altre tipus de contingut (música, pel·lícules, etc.) que no estigui expressament autoritzats.
- Connectar-se a xats, fòrums de discussió, grups de treball o qualsevol aplicació interactiva, així com participar en jocs en línia, que no tinguin relació directa amb les tasques i funcions encomanades.

4.6 ÚS DEL CORREU ELECTRÒNIC

Les característiques del correu electrònic han propiciat l'aparició d'amenaques que utilitzen aquest servei, aprofitant les seves vulnerabilitats, per a propagar-se dins dels sistemes d'informació i serveis de l'FPC. Per aquest motiu s'estableixen les següents directrius amb l'objectiu de reduir el risc en l'ús del correu electrònic:

- El correu electrònic s'ha d'utilitzar exclusivament per a propòsits professionals.
- No s'ha de cedir l'ús del compte de correu a terceres persones.
- És obligatori informar de correus amb virus, *phishing*, *malware* (programa maliciós), etc. sense reenviar-los, per a evitar la seva possible propagació.
- No respondre a missatges d'*spam*.
- Assegurar la identitat del remitent abans d'obrir un missatge.
- No han d'executar-se els arxius adjunts rebuts sense analitzar-los prèviament amb l'eina corporativa contra codi maliciós.

Respecte a l'ús del correu electrònic, queda terminantment prohibit:

- Falsificar, ocultar, suprimir o substituir la identitat de l'emissor en qualsevol correu electrònic.
- Enviar o reenviar missatges amb contingut ofensiu, poc ètic, amenaçador, discriminatori, calumniador o que pugui suposar un deteriorament de la imatge de l'FPC.
- Manipular el contingut de la informació d'un missatge original reenviat, sempre que no s'adverteixi al receptor del tipus de tractament o alteració que se n'ha fet.
- Fer ús del correu electrònic per a la difusió interna o externa de correu no desitjat o correu brossa, virus i codis maliciosos, així com per a l'enviament de cartes en cadena o l'enviament massiu de correus que no tinguin una relació directa amb les tasques i funcions encomanades. L'usuari que, en l'exercici de les seves funcions, hagi de fer enviaments massius de correu ha d'utilitzar les llistes de distribució de correu.
- Llegir o accedir a correus electrònics aliens, sense autorització prèvia.
- Enviar correus electrònics que continguin en el cos o en els adjunts informació amb dades de categories especials de dades o dades especialment sensibles (això és, salut, ideologia, religió, creences, origen racial, ètnic, etc. o aquells considerats com d'especial protecció per l'FPC) tret que es compti amb l'autorització pertinent i s'hagin aplicat les mesures de seguretat oportunes (xifratge).

L'FPC queda facultada per a filtrar el contingut del correu electrònic del compte de correu proporcionat pel desenvolupament de les seves funcions laborals, a fi de prevenir virus o en el cas que existeixin raons fonamentades en una ferma sospita per l'FPC sobre l'existència d'activitats fraudulentament dels usuaris.

El sistema que proporciona el servei de correu electrònic podrà, de manera automatitzada, rebutjar, bloquejar o eliminar part del contingut dels missatges enviats o rebuts en els quals es detecti algun problema de seguretat o d'incompliment de la normativa vigent.

Es podrà inserir contingut addicional en els missatges enviats a fi d'advertir als receptors dels requisits legals i de seguretat que hauran de complir en relació amb aquests correus.

Aquestes directrius també s'hauran de complir amb relació a altres eines de comunicació digital i missatgeria que pugui posar a disposició dels usuaris l'FPC .



4.7 PÈRDUA DE VINCULACIÓ AMB L'ENTITAT

El personal ha de retornar els mitjans electrònics corporatius que custodiï quan perdi la seva vinculació amb l'FPC, o quan es determini que el seu ús ja no és necessari.

El personal s'ha d'abstenir d'esborrar informació dels mitjans electrònics corporatius (xarxa, espais o serveis corporatius, aplicacions corporatives, bústies de correu i suports d'emmagatzematge) quan perdi la seva vinculació amb l'FPC.

Quan un usuari perdi la seva vinculació amb l'FPC, aquesta podrà recuperar la informació dels mitjans electrònics que es van posar a la disposició del personal per a l'exercici de les seves funcions.

4.8 INCIDENTS DE SEGURETAT

Quan es detecti qualsevol anomalia (mal funcionament, aplicacions que no arrenquen o que es tanquen de manera inesperada, pèrdua de documents, etc.) o incident de seguretat (virus, suplantació d'identitat, pèrdua o robatori d'equips o suports, etc.) que pugui comprometre el bon ús i funcionament dels sistemes d'informació de l'FPC o pugui danyar a la seva imatge, haurà d'informar immediatament, fent ús del mecanisme de notificació disponible per l'FPC a través de l'eina de tiquets d'Emotiva o per telèfon al departament de Sistemes depenent de la gravetat.

Durant la gestió d'un incident de seguretat, s'ha d'abstenir de facilitar a tercers qualsevol informació relacionada amb la gestió de l'incident; excepte la informació oficial prevista per l'FPC.

4.9 FORMACIÓ I CONSCIENCIACIÓ

L'FPC s'encarregarà de formar i conscienciar al personal en nocions bàsiques, i específiques, si escau, en matèria de seguretat de la informació, promovent l'enteniment i comprensió de la present norma.

Els usuaris hauran d'atendre el que s'indiqui en les accions de conscienciació i hauran de participar activament a les formacions que l'FPC posi a la seva disposició.

4.10 CONTROL I MONITORATGE

Per a corregir o, si s'escau, exigir responsabilitats, es garantirà que els usuaris estiguin identificats de manera única, de forma que es pugui determinar en tot moment qui rep drets d'accés, de quin tipus són aquests drets i qui ha dut a terme una determinada activitat.

Amb la finalitat de garantir la seguretat, el bon funcionament i la gestió eficient dels sistemes d'informació:

- Es registraran les activitats dels usuaris, retenint la informació estrictament necessària per monitorar, analitzar, investigar i documentar activitats indegudes o no autoritzades, permetent identificar en cada moment la persona que actuï. El registre inclourà l'accés a Internet, les pàgines web visitades, l'hora de connexió i el temps d'accés, el volum de correu electrònic enviat i rebut, així com l'emissor i destinataris dels missatges, l'ús de les comunicacions digitals, el volum de trànsit de descàrrega de dades des d'Internet.
- L'FPC podrà portar a terme taques de control i seguiment, analitzant les comunicacions entrants i sortints, bloquejant i desconnectant qualsevol mitjà electrònic, limitant l'accés a Internet, aplicacions o eines, 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 maliciós així com altres danys a les xarxes i sistemes d'informació.

Les tasques de registre, control i seguiment es portaran a terme de conformitat amb la normativa de protecció de dades, la de funció pública o laboral, els drets fonamentals i la normativa que sigui aplicable, garantint que aquestes mesures seran necessàries i proporcionades amb relació a la finalitat perseguida.

5. DIFUSIÓ

Tots els usuaris dels recursos informàtics i/o sistemes d'informació de l'FPC hauran de tenir accés permanent, durant el temps d'acompliment de les seves funcions, a la present norma.

La norma està disponible a: la intranet Emotiva.

Els usuaris hauran de subscriure el model de l'Annex I, segons que reben el contingut de la norma i es comprometen al seu compliment.

6. GESTIÓ DE LA DOCUMENTACIÓ

Tal com s'estableix en el document que regula la documentació de l'FPC, aquest document serà revisat periòdicament de forma anual pel Responsable de la documentació, o sempre que hi hagi un canvi rellevant a l'FPC, els sistemes d'informació o en la legislació aplicable, que s'encarregarà d'afegir o modificar la documentació oportuna, quan així es requereixi, generant una nova versió.

Qualsevol deficiència i/o inconsistència en aquest document haurà de ser posada en coneixement del Responsable de la documentació.

7. INCOMPLIMENT

Els usuaris han de subjectar les seves actuacions al que estableix aquesta norma. Davant qualsevol ús dels mitjans electrònics que contravinguin el que disposa aquesta norma, sens perjudici que s'adoptin les mesures de restricció o de



suspensió d'ús que considerin escaients, s'exigiran les responsabilitats disciplinàries, patrimonials o de qualsevol altre tipus de responsabilitat que se'n derivin, d'acord amb la legislació vigent, per l'ús deficient o inadequat dels mitjans electrònics.

En el cas d'incompliment de què determina aquesta norma per part del personal extern, s'ha d'aplicar el que estableixi el contracte de prestació de serveis, sens perjudici que l'FPC pugui adoptar les mesures de restricció o suspensió que consideri adients, així com altres mesures orientades a efectuar les reclamacions a les quals aquest incompliment pugui donar lloc.