



**UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH**

Centre Universitari de la Visió

Protocol Intern de seguretat

Drets i Obligacions del Personal i dels estudiants del
CENTRE UNIVERSITARI DE LA VISIÓ en matèria de
Protecció de Dades de Caràcter Personal i Ús de
Recursos Informàtics

Terrassa, Juliol 2018

El present protocol intern de seguretat conté les normes bàsiques de comportament que tot el personal al servei del CENTRE UNIVERSITARI DE LA VISIÓ que tingui accés a dades de persones físiques haurà de complir, així com les normes que regulen l'ús dels recursos informàtics.

Aquestes normes deriven de la necessitat de donar compliment a la normativa de protecció de dades de caràcter personal (Llei orgànica de protecció de dades de caràcter personal i Reglament General de Protecció de Dades) **amb la finalitat de garantir** que cap persona no autoritzada pugui accedir a les dades de persones físiques de les que disposa la UPC i garantir que aquestes dades no puguin ser destruïdes ni alterades sense autorització.

A la present normativa es recullen les normes que han de seguir totes les persones que tenen accés a les dades de caràcter personal estructurades de la següent manera:

1. **Criteris generals de comportament.**
2. **Normes relatives al comportament al lloc de treball.**
3. **Normes relatives a la utilització de recursos informàtics.**
4. **Normes relatives a l'ús del correu electrònic**
5. **Normes relatives a l'accés a internet.**
6. **Propietat intel·lectual i industrial.**
7. **Responsabilitat.**

1.- CRITERIS GENERALS DE COMPORTAMENT

Com a criteri general, les dades de caràcter personal es podran utilitzar única i exclusivament per fer la feina de cadascú, i per tant, queda prohibida qualsevol altra utilització.

Tothom és responsable del seu lloc de treball i dels espais compartits, i per tant, **haurà d'adoptar les mesures necessàries per tal d'impedir l'accés de persones no autoritzades a la informació confidencial**. Això inclou el lloc de treball, entès com el lloc on cadascú realitza la seva feina: despatx, taula, pantalles, impressores; equips informàtics; correu electrònic i l'accés a Internet.

Tota la informació allotjada en els equips, sistemes informàtics i xarxa corporativa de la UPC és de la seva propietat i té caràcter confidencial. Tothom que hi tingui accés haurà de mantenir per temps indefinit la màxima reserva i no podrà divulgar ni utilitzar directament ni mitjançant terceres persones o entitats, dades, documents, metodologies, claus, anàlisis, programes, estudis i altres informacions pertanyents a la UPC, tant en suport de paper com electrònic. Aquesta obligació continuarà vigent fins i tot després de l'extinció de la vinculació amb la UPC.

En particular, no es podrà:

- Crear fitxers de dades personals sense l'autorització del Responsable dels fitxers¹.
- Utilitzar les dades personals per a finalitats diferents d'aquelles per les quals s'hagin recaptat.
- Creuar informació relativa a dades de diferents fitxers o serveis a fi d'establir perfils de personalitat sense autorització del Responsable del fitxer i del Responsable de seguretat¹.

¹ *Figures responsables dels fitxers de la UPC(descrites a l'apartat 1.3.1. del Manual per*

- Utilitzar llistats amb dades de caràcter personal posant en perill la seguretat de les dades. Aquests llistats hauran de romandre sempre a la UPC i no podran sortir sense autorització prèvia del Responsable de Seguretat.
- Obtenir llistats amb dades de caràcter personal sense prèvia autorització del Responsable de Seguretat.
- Realitzar qualsevol altra activitat expressament prohibida en aquest document o en les normes sobre protecció de dades i Instruccions de l'Agència de Protecció de Dades.

2.- NORMES RELATIVES AL COMPORTAMENT AL LLOC DE TREBALL

Entre les mesures de seguretat adoptades per la UPC i que el personal ha de respectar, es troben les següents:

Visualització de les dades per persones no autoritzades:

- Quan algú s'absenti del seu lloc de treball haurà d'impedir l'accés d'altres persones no autoritzades a documents que continguin dades de caràcter personal en pantalla i en paper. Pel que fa als equips informàtics, es pot impedir la visualització mitjançant protectors de pantalla.
- Qui utilitzi una impressora no deixarà documents a la vista de persones no autoritzades. Si els equips són compartits amb altres usuaris no autoritzats hauran de recollir els documents a mesura que es vagin generant.
- No es podran fer còpies dels documents, aquestes hauran de dur-se a terme sota el control del responsable intern del fitxer.
- No es podran treure les dades i els documents fora de les instal·lacions dels CUV.
- Es limitarà la presència de persones externes a les oficines de l'organització, que hauran d'estar sempre acompanyats d'algun intern. Es realitzarà una supervisió i control dels visitants, implicant l'accés als equips informàtics, als arxius manuals o documentació impresa on hi hagi dades de caràcter personal o informació confidencial del CUV.
- Fora de les hores d'oficina, els despatxos es mantindran tancats sota clau i les instal·lacions del CUV es mantindran sempre tancades sota clau i amb alarma.
- Tots els papers que tinguin dades de caràcter personal hauran de desar-se sota clau.

(adequació de la UPC a la normativa reguladora de la Protecció de Dades de Caràcter Personal):

Responsable de fitxer o tractament de la UPC: és la UPC, com a persona jurídica de naturalesa pública, representada pel rector; qui podrà designar com a representant un Vicerector amb competències en política general Tecnologia de la Informàtica i de la Comunicació (TIC), i que marcarà les línies generals sobre polítiques de seguretat.

Responsable de seguretat de la UPC: és la persona o persones nomenades per la UPC a la que el responsable del fitxer ha assignat la funció de coordinar i controlar les mesures de seguretat establertes en el document de seguretat, en la present normativa i en la resta de normativa legal vigent.

L'staff tècnic: format per les persones que tenen funcions d'assessorament en qüestions de tipus legal, posada en marxa de diferents actuacions, seguiment del procés, resposta a les consultes que es puguin plantejar i realització de tasques d'avaluació/auditories que la legislació estableix.

Responsables interns dels fitxers: caps de les unitats o serveis administratius que siguin responsables del tractament de dades dels fitxers de la UPC. Hauran de vetllar perquè el tractament s'ajusti al previst a la legislació així com assegurar-se de l'establiment i compliment de les disposicions de seguretat adient sota el control i supervisió del responsable de seguretat. Pel que fa a les unitats bàsiques (centres docents, departaments o instituts) el "Responsable intern dels fitxers" serà la persona responsable dels serveis econòmics i administratius de la unitat que es tracti.

Administrador de seguretat: Per cada "Responsable intern del fitxer" hi haurà un "Administrador de seguretat", com a responsable operatiu del tractament de dades de cada unitat o servei.

Destrucció o alteració de les dades:

- Ningú pot esborrar, destruir, malmetre, alterar ni modificar les dades de caràcter personal sense l'autorització expressa del Responsable del fitxer, sempre i quan no sigui en exercici de les funcions que li han estat encomanades.
- No es pot llençar a la paperera/escombraries qualsevol document on hi constin dades personals: sempre s'haurà d'utilitzar la destructora de documents o qualsevol altra mitjà similar.

Còpies i comunicacions:

Ningú no pot realitzar còpies, transmissions, comunicacions ni cessions de les dades de caràcter personal propietat del Responsable del fitxer sense l'autorització expressa i escrita d'aquest.

Temporalitat de la possessió de les dades:

En cas que, per motius directament relacionats amb el lloc de treball, hom hagi de disposar d'informació de dades de caràcter personal, s'haurà d'entendre que la possessió d'aquesta informació és estrictament temporal, amb obligació de secret. No tindrà dret a posseir ni podrà fer cap còpia d'aquesta informació.

Així mateix, haurà de tornar els citats materials a la persona que li ha facilitat o destruir-los, immediatament després que finalitzi les tasques que han originat el seu ús temporal.

Connexió a les dades des de fora de la UPC:

No és permès l'accés a les dades de caràcter personal des de fora dels locals de la UPC sense l'autorització expressa del Responsable intern del fitxer, és a dir, del cap del servei o unitat que tracti les dades.

Contrasenya:

S'assignarà a tothom una contrasenya personal i intransferible per accedir als fitxers que continguin dades de caràcter personal.

Aquesta contrasenya té caràcter confidencial, de manera que:

- No està permès revelar-la a ningú sense l'autorització expressa del Responsable del fitxer o del Responsable de Seguretat.
- Es recomana memoritzar-la i no anotar-la enlloc.
- En cas que sigui coneguda per persones no autoritzades s'haurà de canviar i informar-ne al Responsable de Seguretat.
- En cas de no recordar la contrasenya s'haurà de posar en contacte amb el Responsable de Seguretat.

Utilització de suports: disquets, CD-ROM, PEN-DRIVE i altres:

Només les persones autoritzades podran utilitzar disquets, CD-Rom, PEN- DRIVE o qualsevol altre suport per emmagatzemar dades de caràcter personal, en el ben entès que podran extreure els esmentats suports dels locals de la UPC sense prèvia autorització escrita del Responsable de Seguretat.

Altres mesures:

S'ha de respectar qualsevol altra mesura establerta en el present protocol intern o acordada per la UPC per a garantir una major protecció de les dades de caràcter personal enfront d'accessos no autoritzats.

3.- NORMES RELATIVES A LA UTILITZACIÓ DE RECURSOS INFORMÀTICS.

El sistema informàtic és propietat de la UPC. Els usuaris amb accés als sistemes informàtics i de xarxa hauran d'utilitzar-los el més eficientment possible per tal d'evitar el tràfic innecessari i interferències en el treball d'altres usuaris.

Per això, no es podran exercir activitats que consisteixin en:

- Destruir, alterar, inutilitzar o danyar les dades, programes o documents electrònics de la UPC o de tercers.
- Obstaculitzar l'accés d'altres usuaris a la xarxa.
- Trametre missatges de correu electrònic de forma massiva o amb finalitats comercials o publicitàries (SPAM).
- Introduir programes, virus, macros, applets, controls Active X o qualsevol altre dispositiu lògic o seqüència de caràcters que causi o pugui causar qualsevol tipus d'alteració en els sistemes informàtics de la UPC o de tercers.
- Introduir, descarregar d'internet, reproduir, utilitzar o distribuir programes informàtics no autoritzats expressament.
- Instal·lar còpies il·legals de qualsevol programa.
- Utilitzar els recursos telemàtics de la UPC, inclosa la xarxa Internet, per a activitats que no es trobin directament relacionades amb el lloc de treball de l'usuari.
- Introduir continguts obscens, immorals o ofensius i, en general, mancats d'utilitat per als objectius de la UPC, a la xarxa corporativa d'aquesta.
- Transmetre o retransmetre missatges en cadena o de tipus piramidal.
- Intentar distorsionar o falsejar els registres d'activitat històrics (LOG) del Sistema.
- Intentar desxifrar les claus, sistemes o algorismes de xifrat i qualsevol altre element de seguretat que intervingui en els processos telemàtics de la UPC.
- Utilitzar el sistema per intentar accedir a àrees restringides dels sistemes informàtics de la UPC.
- Intentar augmentar el nivell de privilegis d'un usuari en el sistema.

4.- NORMES RELATIVES A L'ÚS DEL CORREU ELECTRÒNIC.

La xarxa corporativa i els terminals utilitzats per cada usuari són propietat de la UPC.

Es considera correu electrònic tant l'intern, entre terminals de la xarxa corporativa, com l'extern, adreçat o provenint d'altres xarxes públiques o privades i especialment Internet.

Cap missatge de correu electrònic serà considerat privat. El seu ús es limitarà estrictament a l'imprescindible per al desenvolupament de l'activitat pròpia de cadascú.

- Qualsevol fitxer introduït a la xarxa corporativa o en el terminal de l'usuari o empleat mitjançant missatges de correu electrònic que provenguin de xarxes externes hauran de complir els requisits establerts en aquestes recomanacions i en especial les relatives a propietat intel·lectual o industrial i a control de virus.
- Es recomana incloure en els missatges de correu electrònic l'avertiment següent:
"Aquest correu electrònic pot contenir informació confidencial o legalment protegida i està exclusivament adreçat a la persona o entitat destinatària. Si vostè

no és el destinatari final o persona encarregada de recollir-lo, no està autoritzat a llegir-lo, retenir-lo, modificar-lo, distribuir-lo, copiar-lo ni a revelar el seu contingut. Si ha rebut aquest correu electrònic per error, li preguem que informi al remitent i elimini del seu sistema el missatge i el material annex que pugui contenir. Gràcies per a la seva col·laboració”.

- Es prohibeix expressament Intentar llegir, esborrar, copiar o modificar els missatges de correu electrònic o arxius d'altres usuaris.
- La UPC, a través de les figures dels Responsables dels fitxers, podrà vigilar, accedir, recuperar i esborrar qualsevol contingut emmagatzemat, creat, rebut o enviat per mitjà de l'ús informàtic del sistema, així com de l'ús del correu electrònic/ internet a través del següent procediment: es notificarà sempre que sigui possible a l'empleat o col·laborador extern i, en tot cas, als representants dels treballadors ara bé, quan la prèvia notificació als empleats i col·laboradors no sigui possible per estar aquests il·localitzables o existeixi risc de pèrdua o destrucció de les dades contingudes al sistema assignat al treballador, tal requisit quedarà convalidat amb la prèvia notificació als representants dels treballadors, produint-se la seva realització en presència d'aquests.
- Si els empleats o col·laboradors usen una contrasenya per accedir a qualsevol dels sistemes de correu electrònic/telèfon/internet, o encripten els seus missatges no disminuiran els drets de la UPC a accedir al material existent en els seus sistemes, ni es crearà cap dret privat dels empleats respecte dels missatges i fitxers continguts als sistemes. Qualsevol contrasenya usada pels empleats o col·laboradors ha de ser revelada al Responsable intern del fitxer si aquest ho sol·licita, per tal que pugui accedir als fitxers dels sistemes de correu i de veu.
- No es pot crear, ni enviar cap missatge ni de correu electrònic ni telefònic si conté material intimidatori, hostil, o ofensiu concernent a sexe, raça, color, nacionalitat d'origen, religió, orientació sexual, edat o discapacitat, relacionat amb un altre empleat o col·laborador de la companyia, o amb qualsevol altra característica protegida per la llei o les polítiques de la UPC. Quan algú rebí un missatge amb aquests continguts haurà de prendre les mesures necessàries per evitar-ho.
- Els sistemes de correu electrònic/telèfon/Internet no poden ser utilitzats per a promoure causes polítiques ni religioses, empreses comercials, organitzacions externes ni altres peticions no relacionades amb el treball.
- Qualsevol empleat o col·laborador que descobreixi un ús incorrecte dels sistemes de correu electrònic/telèfon/Internet ho haurà de comunicar immediatament al Responsable de Seguretat i responsable de personal de la UPC.
- En relació als incompliments de la política sobre els sistemes de correu electrònic/telèfon/Internet s'aplicarà el que s'estableix a l'apartat 7 d'aquest document.
- Queda prohibit comunicar a una altra persona l'identificador d'usuari i la clau d'accés. Si l'usuari sospita que una altra persona coneix les seves dades d'identificació i d'accés, haurà de posar-ho en coneixement del responsable del sistema, a fi que li assigni una nova clau. Davant d'una baixa o absència temporal de l'usuari, el cap del servei o unitat podrà sol·licitar al responsable del sistema la cessió de clau o dades a la persona per ell designada.

5.- NORMES RELATIVES A L'ACCÉS A INTERNET

Les activitats permeses a Internet són aquelles relacionades amb l'activitat que s'exerceix a la UPC.

- L'ús del sistema informàtic de la UPC per accedir a pàgines web (www), grups de notícies i altres fonts d'informació, es limitarà a l'obtenció d'informació relacionada amb l'activitat de la UPC i escaient del lloc de treball de l'usuari o empleat.
- L'accés en temps real a debats a través de programes de Xat pot ser perillós per facilitar la instal·lació d'utilitats que podrien permetre accessos no autoritzats al sistema; és per això que la recomanació general és de no accedir-hi. L'ús d'altres sistemes de comunicació instantània per a funcions relacionades amb l'activitat de la UPC es podrà fer quan es disposi d'una adequada configuració que garanteixi els nivells de seguretat de la UPC.
- El Responsable del fitxer es reserva el dret de monitoritzar i comprovar, de forma aleatòria i sense previ avís, qualsevol sessió d'accés a internet iniciada per un usuari de la xarxa corporativa.

6.- PROPIETAT INTEL·LECTUAL I INDUSTRIAL.

No està permès l'ús de programes informàtics sense la corresponent llicència, així com l'ús, reproducció, cessió, transformació o comunicació pública de qualsevol tipus d'obra o d'invenió protegida per la propietat intel·lectual o industrial.

7.- RESPONSABILITAT.

L'incompliment de les obligacions per part del personal serà sancionat disciplinàriament, prèvia instrucció del preceptiu expedient.

De la mateixa manera, sense perjudici de la responsabilitat disciplinària en què pugui incórrer el personal, s'exigirà d'ofici la corresponent responsabilitat pels danys i perjudicis ocasionats als particulars, sempre que hagi existit dol o culpa greu.

La responsabilitat penal i la responsabilitat civil derivada del delicte en què hagi incorregut el personal, s'exigirà de conformitat amb la legislació corresponent.