Institut de Formació Contínua-IL3
UNIVERSITAT DE BARCELONA

POLÍTICA DE SEGURETAT DEL PERSONAL

1.- ÀMBIT D'APLICACIÓ.

FUNDACIÓ INSTITUT DE FORMACIÓ CONTÍNUA DE LA UNIVERSITAT DE BARCELONA (d´ara endavant IL3), com a Responsable del tractament, es compromet a implantar una cultura de privacitat, seguretat i compliment de la normativa de Protecció de Dades de Caràcter Personal (d'ara endavant, PDCP) en l'organització, i per poder fer-ho és necessari que el personal d'aquesta entitat local i que estigui autoritzat a tractar dades de caràcter personal estigui degudament informat de la Política de Seguretat en el tractament de dades i se'n responsabilitzi. La Política de Seguretat plasmada en aquest document s'adreça a tot el personal de la institució, que estigui degudament autoritzat per tractar dades de caràcter personal i al qual se li exigeix que la llegeixi, comprengui, compleixi i la faci complir amb la finalitat de protegir les dades de caràcter personal que formen part del tractament que li ha estat encomanat.

Independentment de l'obligat compliment del Reial Decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració Electrònica -d'ara endavant, E.N.S-, aquesta Política de seguretat estableix les obligacions i procediments que ha seguir el personal laboral que efectuï un tractament de dades de caràcter personal en el desenvolupament de la seva activitat i es fonamenta en el que disposa el vigent Reglament (UE) 2016/679 del Parlament Europeu i de Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa a el tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE Reglament general de protecció de dades- (d'ara endavant, RGPD); en la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals (d'ara endavant, LOPDGDD); i en la resta de normativa concordant aplicable.

En aquest sentit, per vetllar pel compliment d'aquesta Política, IL3 ha assignat funcions/designat un Responsable de seguretat que estarà a disposició de tot el personal i s'encarregarà de coordinar, controlar, desenvolupar i verificar que es compleixin les normatives esmentades. També ha procedit al nomenament d'un Delegat de Protecció de Dades -DPD-.

Responsable de Seguretat Informàtica. Martin Madueño Ortega , correu mmadueno@il3.ub.edu.
Responsable dep. Legal. Marta Garcia Sampietro, correu magarcia@il3.ub.edu
Delegat de Protecció de Dades (DPO): Sergio Girona Barroso, correu dpd@il3.ub.edu

2.- CONCEPTES BÀSICS

Per proporcionar una millor comprensió de la protecció de dades, de conformitat amb l'article 4 RGPD, definim els principals conceptes bàsics:

Estructura del tractament:

- **Dades personals**: Qualsevol informació sobre una persona física identificada o identificable.

- **Tractament**: Qualsevol operació o conjunt d'operacions realitzades sobre dades personals o conjunts de dades personals, ja sigui per procediments automatitzats o no, com la recollida, el registre, l'organització, l'estructuració, la conservació, l'adaptació o la modificació, l'extracció, la consulta, la utilització, la comunicació per transmissió, difusió o qualsevol altra forma d'habilitació d'accés, acarament o interconnexió, limitació, supressió o destrucció.
- **Interessat**: Persona física identificada o identificable sotmesa al tractament de les seves dades personals.
- **Persona física identificable:** Qualsevol persona la identitat de la qual es pot determinar, directament o indirectament, en particular mitjançant un identificador, com ara un nom, un número d'identificació, dades de localització, un identificador en línia o un o diversos elements propis de la identitat física, fisiològica, genètica, psíquica, econòmica, cultural o social d'aquesta persona.
- **Fitxer**: Qualsevol conjunt estructurat de dades personals, accessibles d'acord amb criteris determinats, ja sigui centralitzat, descentralitzat o repartit de forma funcional o geogràfica.
- **Responsable del tractament**: La persona física o jurídica, autoritat pública, servei o un altre organisme que, sol o juntament amb altres, determini les finalitats i mitjans del tractament.
- **Personal autoritzat**: Persona autoritzada pel Responsable per efectuar un tractament de dades mitjançant un compromís de confidencialitat.

Categories de dades:

- **Bàsiques**: Dades que no corresponguin a categories Penals o Especials, per exemple: nom, adreça, e-mail, número de telèfon, edat, sexe, firma, imatge, aficions, patrimoni, dades bancàries, informació acadèmica, professional, social, financera, etc.
- **Penals**: Dades relatives a la comissió d'infraccions administratives o penals, o dades que puguin oferir una definició de característiques de personalitat, etc.
- **Especials**: Dades relatives a l'origen ètnic o racial, opinions polítiques, conviccions religioses o filosòfiques, afiliació sindical, dades genètiques o biomètriques que permetin la identificació unívoca d'una persona, dades relatives a la salut o a la vida i orientació sexuals.

3.- PRINCIPIS DE LA PROTECCIÓ DE DADES

Els principis fonamentals per efectuar un tractament de dades són:

- **Licitud**: Lleialtat i transparència amb l'interessat.
- **Limitació de les finalitats**: Tractades per a finalitats determinades.
- **Minimització de les dades**: Només s'han d'obtenir les dades necessàries per assolir les finalitats.
- **Exactitud**: Actualitzades.
- **Limitació del termini de conservació**: Guardades no més temps del necessari per aconseguir les finalitats.
- **Integritat i confidencialitat**: Aplicació de mesures de seguretat per a la protecció de dades en totes les fases del tractament.

- **Responsabilitat proactiva**: S'ha de poder demostrar el compliment de tots els principis de protecció de dades.

Licitud del tractament de dades de caràcter personal

El tractament de dades de caràcter personal només és lícit si es compleix a almenys una de les següents condicions:

- L'interessat ha donat el seu consentiment exprés per al tractament de les seves dades personals per a una o diverses finalitats específiques i es procedeix a guardar el document probatori que ho acrediti.
- El tractament és necessari per executar un contracte en el qual l'interessat és part o bé per aplicar mesures precontractuals a petició seva.
- El tractament és necessari per complir una obligació legal aplicable al responsable del tractament.
- El tractament és necessari per protegir interessos vitals de l'interessat o d'una altra persona física.
- El tractament és necessari per satisfer interessos legítims perseguits pel responsable del tractament o per un tercer, sempre que no hi prevalguin els interessos o els drets i les llibertats fonamentals de l'interessat que requereixen la protecció de dades personals, especialment si l'interessat és un nen.
- El tractament és necessari per complir una missió efectuada en interès públic o en l'exercici de poders públics conferits al responsable del tractament.

Informació del tractament a l'interessat.

Cal facilitar la següent informació a l'interessat:

- La identitat i les dades de contacte del Responsable del tractament.
- Les dades de contacte del delegat de protecció de dades de IL3.
- Les finalitats o la finalitat del tractament.
- La base jurídica del tractament.
- Els destinataris de les dades.
- Si es preveu la transferència internacional de dades.
- El termini de conservació de les dades o els criteris que ho determinin.
- Els drets que té l'interessat.
- Forma de reclamació de drets i dades de contacte de l'autoritat de control.
- I si les dades no s'han obtingut de l'interessat:
    - Categoria de dades.
    - Fonts de procedència.

Responsabilitat del tractament.

En alguns supòsits, pot ser que el tractament de dades sigui efectuat per encarregats del tractament o destinataris de les dades, sempre que hi hagi un mandat legal o una autorització expressa del

Responsable i s'hagi formalitzar un contracte per efectuar aquest tractament d'acord amb la legislació vigent.

- **Encarregats del tractament**: La persona física o jurídica, autoritat pública, servei o un altre organisme que tracti dades personals per compte del responsable del tractament.
- **Destinataris de dades**: La persona física o jurídica, autoritat pública, servei o qualsevol altre organisme al qual es comuniquen dades personals, tant si és un tercer com si no. No obstant això, no es consideren destinataris les autoritats públiques que puguin rebre dades personals en el marc d'una investigació concreta de conformitat amb el Dret de la Unió o dels Estats membres. El tractament d'aquestes dades efectuat per aquestes autoritats públiques és conforme a les normes en matèria de protecció de dades que són d'aplicació a les finalitats del tractament.

Per conèixer més informació sobre encarregats del tractament o destinataris de dades, han d'enviar una sol·licitud justificada adreçada al Responsable de seguretat.

Mesures de seguretat.

IL3 ha implementat mesures tècniques i organitzatives per garantir un nivell de seguretat adequat als riscos que pugui comportar el tractament com a conseqüència de la destrucció accidental o il·lícita de dades, la pèrdua, alteració o comunicació no autoritzada i l'accés a les dades quan són transmeses, conservades o objecte d'algun altre tipus de tractament.

El personal ha de vetllar per la seguretat de les dades tractades per l'administració i comunicar al Responsable o al Delegat de Protecció de Dades qualsevol operació de tractament que pugui comportar un risc que afecti la protecció de dades o els interessos i llibertats dels interessats.

Qualsevol disseny d'una nova operació de tractament o actualització d'una operació existent ha de comptar amb la participació del Delegat de Protecció de Dades i garantir abans d'implantar-se la protecció de dades personals i l'exercici dels drets dels interessats en totes les fases del tractament: obtenció, accés, intervenció, transmissió, conservació i supressió.

Esquema Nacional de Seguretat.

L'E.N.S es constitueix pels principis bàsics i requisits mínims requerits per a una protecció adequada de la informació. Serà aplicat per les administracions públiques per assegurar l'accés, integritat, disponibilitat, autenticitat, confidencialitat, traçabilitat i conservació de les dades, informacions i serveis utilitzats en mitjans electrònics que gestionin en l'exercici de les seves competències

La finalitat de l'E.N.S és la creació de les condicions necessàries de confiança en l'ús dels mitjans electrònics, a través de mesures per garantir la seguretat dels sistemes, les dades, les comunicacions i els serveis electrònics, que permeti als ciutadans i a les Administracions públiques l'exercici de drets i el compliment de deures a través d'aquests sistemes.

L'E.N.S persegueix fonamentar la confiança en què els sistemes d'informació proporcionaran els seus serveis i custodiaran la informació d'acord amb les seves especificacions funcionals, sense interrupcions o modificacions fora de control, i sense que la informació pugui arribar a persones no autoritzades. Es desenvoluparà i perfeccionarà en paral·lel a l'evolució dels serveis i a mesura que es vagin consolidant els requisits d'aquests i de les infraestructures que ho recolzen.

Actualment els sistemes d'informació de les administracions públiques estan fortament imbricats entre si i amb sistemes d'informació del sector privat: empreses i administracions. D'aquesta manera, la seguretat té un nou repte que va més enllà de l'assegurament individual de cada sistema. És per això que cada sistema ha de tenir clar el seu perímetre i els responsables de cada domini de seguretat s'han de coordinar efectivament per evitar «terres de ningú» i fractures que poguessin danyar la informació o els serveis prestats.

En aquest context s'entén per seguretat de les xarxes i de la informació la capacitat de les xarxes o dels sistemes d'informació de resistir, amb un determinat nivell de confiança, els accidents o les accions il·lícites o malintencionades que comprometin la disponibilitat, autenticitat, integritat i confidencialitat de les dades emmagatzemades o transmeses i dels serveis que les esmentades xarxes i sistemes ofereixen o fan accessibles.

Segons l'article 5 de l'E.N.S, la seguretat s'entén com un procés integral constituït per tots els elements tècnics, humans, materials i organitzatius relacionats amb el sistema. L'aplicació de l'Esquema Nacional de Seguretat està presidida per aquest principi, que exclou qualsevol actuació puntual o tractament conjuntural. S'ha de prestar la màxima atenció a la conscienciació de les persones que intervenen en el procés i als seus responsables jeràrquics, perquè, ni la ignorància, ni la falta d'organització i coordinació, ni instruccions inadequades siguin fonts de risc per a la seguretat.

4 - FUNCIONS I OBLIGACIONS DEL PERSONAL

El personal ha d'actuar en tot moment d'acord amb les instruccions que es detallen a l'acord de confidencialitat subscrit amb l'organització i les que estableix aquesta Política de seguretat. Per aquest motiu, s'estableixen, a continuació, les mesures de protecció de dades que el personal es compromet a complir expressament:. A més, han de respectar els mandats de confidencialitat, secret professional i el que estableix l'Esquema Nacional de Seguretat (d'ara endavant, E.N.S) i en aquesta Política de seguretat. Per això, sense perjudici de complir el que estableix l'E.N.S, es disposen les següents mesures de protecció de dades que el personal també ha de complir expressament:

Organització de la informació.

S'han de classificar les dades de caràcter personal de manera que es puguin exercir els drets dels interessats: Accés, rectificació, supressió i portabilitat de les dades, i limitació o oposició al tractament.

Conservació de les dades.

S'han de conservar les dades en el mobiliari i departaments destinats per a aquesta finalitat. Per a tractaments automatitzats, cal guardar els arxius als suports, carpetes o directori de xarxa que indiqui el Responsable de seguretat.

No és permès de conservar dades a l'escriptori físic o digital. Només se'n permet el tractament temporal a l'escriptori per efectuar les operacions que ho requereixin, sempre que es conservin al lloc adequat en finalitzar la jornada laboral.

Accés a la informació.

S'han d'aplicar els mecanismes d'accés restringit a la informació que hagi implementat IL3 i salvaguardar les claus d'accés de tota divulgació o comunicació a altres persones.

Cada empleat només està autoritzat a accedir als recursos que siguin necessaris per al desenvolupament i compliment de les seves tasques i/o funcions.

Cal restringir l'accés als equips informàtics mitjançant procediments que puguin identificar i autenticar l'empleat que hi accedeixi. Els noms d'usuari i les contrasenyes tenen consideració de dades personals intransferibles i personalíssimes.

Processament de dades.

Els suports documentals i informàtics han d'estar disposats de tal manera que no siguin accessibles a persones o empleats no autoritzats.

Si un empleat abandona el seu lloc de treball temporalment, ha d'amagar els documents i bloquejar l'ordinador, de manera que s'impedeixi visualitzar la informació amb què està treballant.

Quan s'utilitzin impressores o fotocopiadores, després de la impressió de treballs amb informació de caràcter personal, cal recollir-los immediatament, o imprimir de forma bloquejada, i assegurar-se de no deixar documents impresos a la safata de sortida.

Registre d'activitat.

En els supòsits d'aplicació de l'E.N.S, de conformitat amb el que disposa l'article 23, amb la finalitat exclusiva d'aconseguir el compliment de l'objecte de l'esmentada norma i 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 siguin d'aplicació, es registraran les activitats dels usuaris, tot retenint la informació necessària per monitoritzar, analitzar, investigar i documentar activitats indegudes o no autoritzades, per tal de permetre identificar en cada moment la persona que actua.

Transport de suports.

El transport de suports (ordinadors portàtils, pendrives, discs durs, carpetes físiques amb documents...) que continguin dades personals només el poden dur a terme els empleats autoritzats o empreses externes contractades per a aquesta finalitat pel Responsable del tractament.

Eliminació de documents.

Qualsevol document físic o suport digital que s'hagi d'eliminar i que inclogui dades personals s'ha de destruir amb la destructora o ha de ser retirat per una empresa homologada de destrucció de documents. En els supòsits de dubte o manca dels anteriors elements, l'empleat podrà adreçar-se al Delegat de Protecció de Dades per fer arribar la seva consulta sobre la manera més adequada de procedir a l'eliminació de documents per garantir el compliment de la normativa de protecció de dades.

Còpia de seguretat i recuperació de dades.

Els empleats han d'emmagatzemar tota la informació tractada al directori de xarxa o administració electrònica corresponent indicada pel Responsable de seguretat, la qual cosa permetrà que s'hi apliquin les mesures de seguretat existents i que es duguin a terme els procediments de còpies de seguretat aplicats per l'organització.

Protecció de dades.

S'han d'aplicar les mesures de protecció i seguretat de dades que estableix l'Administració en l'E.N.S i les relatives amb la seguretat del tractament, com ara la pseudonimització o xifratge de dades o advertències d'intrusió com antivirus, antispam, etc.

Gestió d'incidències, violació de seguretat o forats de seguretat de les dades personals.

Es considera una incidència, violació de seguretat o forat de seguretat de les dades personals qualsevol incident de seguretat que provoqui la destrucció, pèrdua o alteració accidental o il·lícita de dades personals transmeses, conservades o tractades d'una altra manera, o la comunicació o accés no autoritzat a aquestes dades.

Les empleades i empleats, de manera immediata i fefaent, tenen l'obligació de notificar al Responsable de seguretat o al Delegat de Protecció de Dades l'existència de qualsevol incidència, violació de seguretat o forat de seguretat de la qual tinguin constància. Cal aplicar la consideració anterior per tal d'assegurar el coneixement i correcta aplicació de mesures correctores tendents a posar remei i mitigar els efectes que hagi pogut ocasionar.

Les incidències, violacions de seguretat o forats de seguretat s'han de documentar al més aviat possible per la persona que la notifica amb una descripció detallada i la data i hora en què s'ha produït o se n'ha tingut constància.

FUNCIONS I OBLIGACIONS DE COMPLIMENT OBLIGATORI.

Els USUARIS són totes les persones que exerceixen funcions sota l'autoritat de IL3 que intervenen en el tractament de qualsevol informació generada per l'organització relativa tant a dades personals com a altres tipus de dades. Els USUARIS han d'actuar d'acord amb l'específica normativa establerta en la matèria per a la funció pública i en les instruccions contemplades en l'Acord de confidencialitat i secret professional, i s'han de comprometre a més a complir les funcions i obligacions relacionades en aquest annex.

I. Confidencialitat de la informació

Resten **expressament prohibides** les següents activitats:

1. Enviar a l'exterior o revelar a tercers informació que no hagi estat declarada com a no confidencial per IL3, mitjançant qualsevol procediment o suport, ja sigui electrònic, digital, manual o documental, o a través de qualsevol altre mitjà de comunicació, inclosa la simple visualització o accés a aquesta.
2. L'ús de càmeres fotogràfiques, de vídeo, de so o qualsevol instrument que pugui emmagatzemar informació audiovisual, que no hagi estat facilitada per IL3 per complir amb unes finalitats específiques.
3. Divulgar directament o a través de terceres persones o empreses les dades, documents, metodologia, claus, anàlisis, programes i altres informacions a les quals tinguin accés durant la seva relació laboral o professional amb l'organització, ja sigui en suport material com electrònic. Aquesta prohibició continuarà vigent després de l'extinció del contracte laboral per temps indefinit, amb excepció d'aquells casos en els que sigui requerit per imperatiu legal.
4. Disposar, per utilitzar fora de la seva responsabilitat, de material o informació propietat de IL3 o del seu client en el qual es duguin a terme els serveis, tant en l'actualitat com en el futur.

En cas que, per motius directament relacionats amb el lloc de treball, l'USUARI acabi en possessió d'informació que no hagi estat declarada com a no confidencial per part de IL3, en qualsevol tipus de suport, s'ha d'entendre que aquesta possessió és estrictament temporal, amb obligació de secret i sense que això li atorgui cap dret de possessió, o titularitat o còpia sobre la informació esmentada.

Així mateix, l'USUARI ha de retornar aquests materials a IL3 immediatament després de finalitzar les tasques que n'han originat l'ús temporal i, en qualsevol cas, en finalitzar la relació laboral o professional. L'ús continuat de la informació en qualsevol format o suport de diferent manera de la pactada i sense consentiment de IL3, no ha de comportar, en cap cas, una modificació d'aquesta clàusula.

L'incompliment d'aquestes obligacions pot constituir un delicte de revelació de secrets, previst en els articles 197 i 278 del Codi Penal, i donar dret a IL3 a procedir com estimi oportú en defensa dels seus interessos i a exigir a l'usuari responsabilitat patrimonial, tant pels danys causats a particulars com a la mateixa Institució. La consideració anterior és sens perjudici de qualsevol altre mecanisme que prevegi a l'efecte l'ordenament jurídic o les normes sectorials d'aplicació.

II. Ús dels sistemes informàtics (SI)

El Sistema Informàtic, i els terminals utilitzats per cada usuari són, amb caràcter general, propietat de IL3.

Resten **expressament prohibides** les següents activitats:

1. L'ús de programes informàtics sense la llicència corresponent, així com l'ús, reproducció, cessió, transformació o comunicació pública de qualsevol tipus d'obra o invenció protegida per la propietat intel·lectual o industrial. L'incompliment podrà ser causa de responsabilitat disciplinària, administrativa, civil i penal.
2. Destruir, alterar, inutilitzar o danyar de qualsevol altra manera les dades, programes o documents electrònics de IL3 o de tercers. Aquests actes poden constituir un delicte de danys, previst a l'article 264.2 del Codi Penal.
3. Introduir voluntàriament programes, virus, macros, applets, controls ActiveX o qualsevol altre dispositiu lògic o seqüència de caràcters que causin o siguin susceptibles de causar qualsevol tipus d'alteració en els Sistemes Informàtics de IL3 o de tercers. Sobre aquest tema, cal recordar que el propi sistema executa automàticament els programes antivirus i les actualitzacions per prevenir l'entrada al sistema de qualsevol element destinat a destruir o corrompre les dades informàtiques.
4. Introduir, descarregar d'Internet, reproduir, utilitzar o distribuir programes informàtics no autoritzats expressament per IL3. Aquesta prohibició inclou qualsevol altre tipus d'obra o material els drets de propietat intel·lectual o industrial dels quals pertanyin a tercers, en cas que no es disposi d'una autorització.
5. Instal·lar còpies il legals de qualsevol programa, inclosos els que estiguin estandarditzats.
6. Esborrar qualsevol programa instal·lat de manera legal.
7. Introduir contingut obscens, immorals o ofensiu i, en general, que manquin d'utilitat per als objectius de IL3.
8. Xifrar informació sense estar-hi expressament autoritzat.

III. Salvaguarda i protecció de les contrasenyes personals

Resten **expressament prohibides** les següents activitats:

1. Compartir o facilitar l'identificador d'usuari i la clau d'accés (contrasenya) proporcionats per IL3 a una altra persona física o jurídica. Si l'USUARI sospita que una altra persona coneix les seves dades d'identificació i accés, ha de notificar aquesta incidència al Responsable de seguretat per activar els mecanismes de canvi de contrasenya. En cas d'incompliment d'aquesta obligació, l'USUARI serà l'únic responsable dels actes realitzats per la persona física o jurídica que utilitzi de manera no autoritzada la seva identificació.

2. Intentar distorsionar o falsejar els registres log del sistema.
3. Intentar augmentar o disminuir el nivell de privilegis d'un USUARI en el sistema sempre que això no formi part de les funcions que té expressament assignades a IL3.

IV. Accés a xarxes

Resten **expressament prohibides** les següents activitats:

1. Utilitzar les dades, la xarxa corporativa i/o la intranet de IL3 i/o de tercers per incórrer en activitats que puguin considerar-se il·lícites o il·legals, que infringeixin els drets de l'organització i/o de tercers o que puguin atemptar contra la moral o les normes d'etiqueta de les xarxes telemàtiques.
2. Intentar desxifrar les claus, sistemes o algoritmes de xifrat i qualsevol altre element de seguretat que intervingui en els processos telemàtics de IL3.
3. Utilitzar el sistema per intentar accedir a àrees restringides dels sistemes informàtics de IL3 i/o de tercers.
4. Emmagatzemar prolongadament informació en el disc local o en suports externs. La informació només es pot emmagatzemar en els espais habilitats a aquest efecte, llevat que el Responsable de Seguretat Informàtica en tingui coneixement i ho autoritzi expressament.
5. Obstaculitzar voluntàriament l'accés dels altres USUARIS a la xarxa mitjançant el consum massiu dels recursos informàtics i telemàtics de l'organització, així com realitzar accions que danyin, interrompin o generin errors en aquests sistemes.

V. Recursos telemàtics i accés a Internet

La connexió a Internet, que s'ha de fer únicament mitjançant la xarxa corporativa habilitada amb aquest efecte, es justifica per finalitats professionals i exclusivament per al compliment de les funcions i tasques assignades.

IL3 es reserva el dret de monitorar i comprovar, de manera aleatòria i sense previ avís, qualsevol sessió d'accés a Internet iniciada per un USUARI.

Qualsevol arxiu introduït als Sistemes Informàtics des d'Internet, ha de complir els requisits establerts en aquestes normes i, en especial, en les que fan referència a la propietat intel·lectual i al control de virus.

Per tal de protegir la informació de l'estació de treball i d'evitar la sobrecàrrega de la xarxa, llevat dels casos relacionats directament amb les funcions encomanades, estan expressament prohibides, ja sigui dins o fora de la seva jornada de treball, les accions següents:

1. Consultar pàgines web que no tinguin relació directa amb les funcions i tasques assignades, incloent-hi pàgines web de vídeos en línia.
2. Descarregar fitxers o programes que no estiguin justificats en l'exercici de les seves funcions i tasques encomanades, incloent-hi música, vídeo i jocs.
3. Connectar-se a xats, fòrums de discussió, grups de treball o qualsevol aplicació interactiva, així com participar en jocs en línia.

VI. L'ús del correu electrònic i missatgeria

Es considera correu electrònic tant l'intern com l'extern, dirigit o provinent d'altres xarxes privades o públiques, especialment Internet.

IL3 es reserva el dret de revisar, sense previ avís, els missatges de correu electrònic dels USUARIS de la xarxa corporativa i els arxius log del Sistema Informàtic, amb la finalitat de comprovar el compliment d'aquestes normes i prevenir activitats que puguin afectar l'organització com a responsable civil subsidiari.

Qualsevol fitxer introduït als Sistemes Informàtics a través de missatges de correu electrònic, provinents de xarxes externes, ha de complir els requisits que s'estableixen en aquestes normes a més de les del client, en especial, les que fan referència a propietat intel·lectual i industrial i a control de virus.

Les adreces de correu electrònic dirigides a persones es consideren dades personals, per la qual cosa, en cas d'enviar correus a més d'un destinatari, si no és estrictament necessari que els altres vegin les adreces de correu de la resta, cal fer-ho com a còpia oculta «Cco».

Estan **expressament prohibides** les següents activitats:

1. Intentar llegir, esborrar, copiar o modificar els missatges de correu electrònic o arxius d'altres USUARIS. Aquesta activitat pot constituir un delicte d'intercepció de les telecomunicacions (revelació de secrets), previst a l'article 197 del Codi penal.
2. Enviar missatges de correu electrònic de manera massiva o amb finalitats comercials o publicitàries sense el consentiment del destinatari.
3. Enviar o reenviar missatges en cadena o de tipus piramidal.

VII. Tractament de la informació

Resten **expressament prohibides** les següents activitats:

1. Accedir a recursos que no siguin necessaris per al desenvolupament i compliment de la seva labor, així com consultar, copiar, reproduir, transmetre, editar, modificar o eliminar informació sense estar autoritzat per a aquestes funcions.
2. Utilitzar impressores o fotocopiadores sense recollir immediatament els documents impresos de la safata de sortida, per tal d'evitar que altres persones no autoritzades puguin accedir a la informació.

3. Destruir qualsevol document físic o suport digital que contingui dades personals sense utilitzar la destructora de paper o sense guardar-los degudament custodiats fins que siguin retirats per una empresa homologada de destrucció de documents.
4. No bloquejar la pantalla de l'ordinador en abandonar temporalment el lloc de treball, de manera que s'impedeixi que persones no autoritzades en vegin la informació.

VIII. Gestió d'incidències

És obligació del personal, com a USUARI, comunicar a IL3 en el menor termini possible totes les incidències, violacions de seguretat o forats de seguretat que es produeixin en l'organització, enteses aquestes com qualsevol incident de seguretat que provoqui la destrucció, pèrdua o alteració accidental o il·lícita de dades personals transmeses, conservades o tractades d'una altra manera, o la comunicació o accés no autoritzat a aquestes dades, també té aquesta consideració l'incompliment de les obligacions detallades en aquest document.

Aquesta comunicació ha d'incloure la identificació clara de la incidència, violació de seguretat o forat de seguretat i una descripció detallada; que ha de contenir, com a mínim: el moment –dia i hora– en què s'ha produït, la persona que n'ha tingut constància, les persones a les quals s'ha comunicat, els efectes produïts i les mesures correctores adoptades.